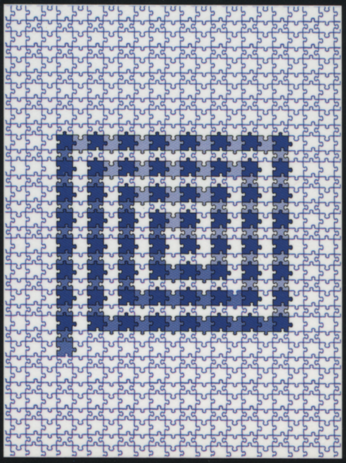
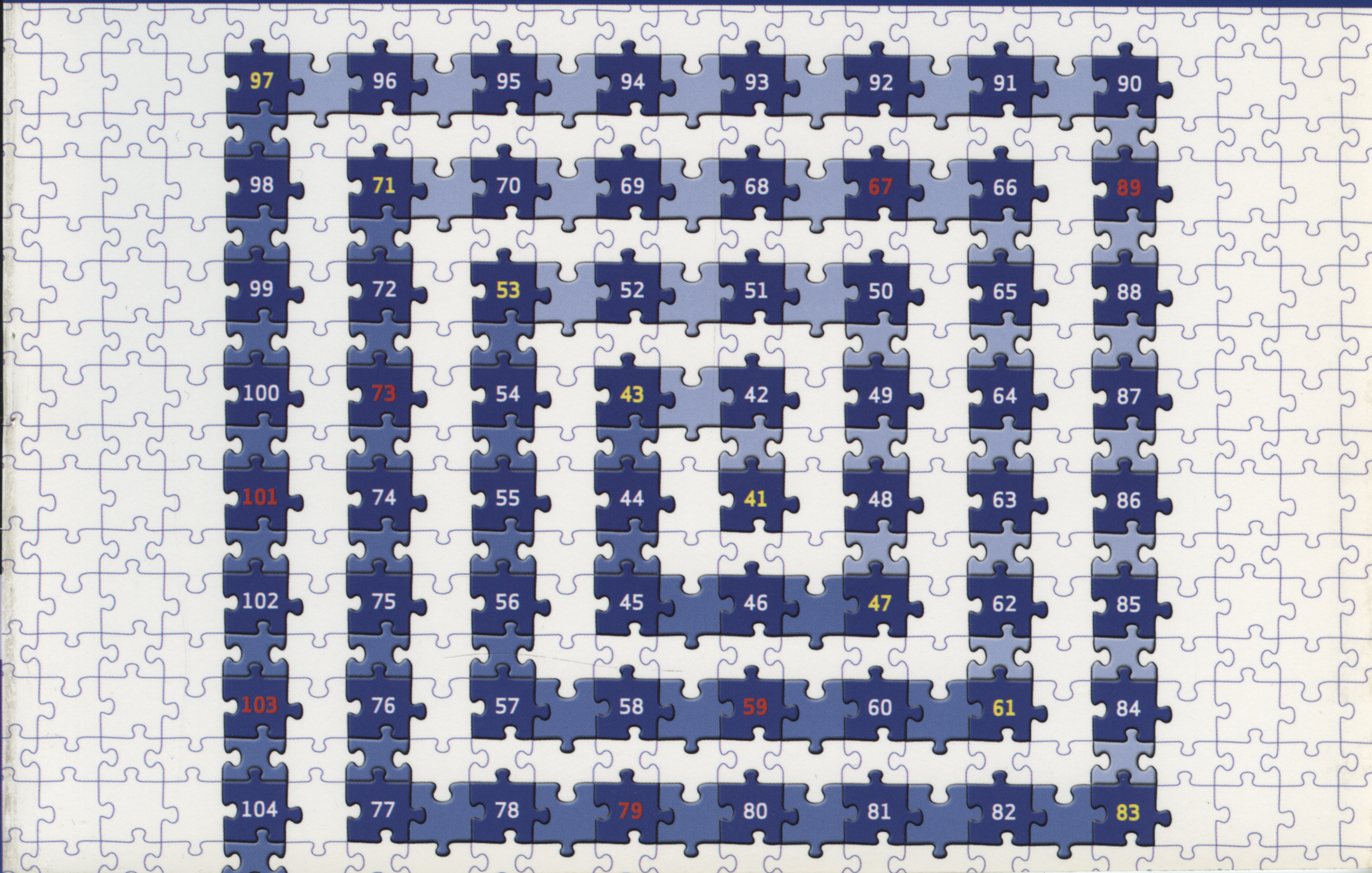
The Open University

M381 Number Theory and
Mathematical Logic



Number Theory **Unit 2**

Prime Numbers


97 96 95 94 93 92 91 90
98 71 70 69 68 67 66 89
99 72 53 52 51 50 65 88
100 73 54 43 42 49 64 87
101 74 55 44 41 48 63 86
102 75 56 45 46 47 62 85
103 76 57 58 59 60 61 84
104 77 78 79 80 81 82 83

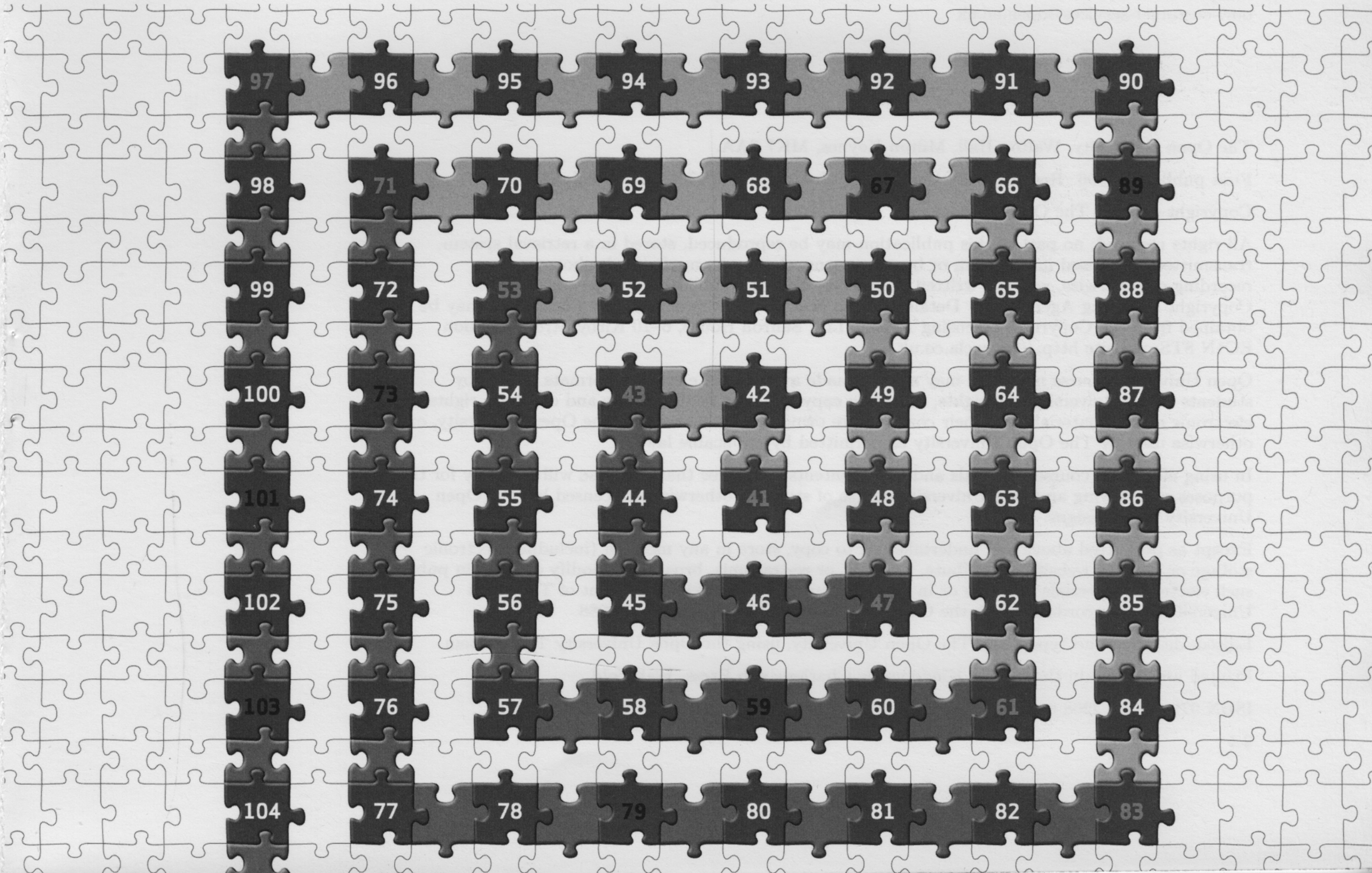
The Open University

M381 Number Theory and Mathematical Logic

Number Theory **Unit 2**

Prime Numbers

Prepared for the Course Team by Alan Best


97 96 95 94 93 92 91 90
98 71 70 69 68 67 66 89
99 72 53 52 51 50 65 88
100 73 54 43 42 49 64 87
101 74 55 44 41 48 63 86
102 75 56 45 46 47 62 85
103 76 57 58 59 60 61 84
104 77 78 79 80 81 82 83

The M381 Number Theory Course Team

The Number Theory half of the course was produced by the following team:

Alan Best	*Author*
Andrew Brown	*Course Team Chair* and *Academic Editor*
Roberta Cheriyan	*Course Manager*
Bob Coates	*Critical Reader*
Dick Crabbe	*Publishing Editor*
Janis Gilbert	*Graphic Artist*
Derek Goldrei	*Critical Reader*
Caroline Husher	*Graphic Designer*
John Taylor	*Graphic Artist*

with valuable assistance from:

CMPU	*Mathematics and Computing, Course Materials Production Unit*
John Bayliss	*Reader*
Elizabeth Best	*Reader*
Jeremy Gray	*History Reader*
Alison Neil	*Reader*

The external assessor was:

Alex Wilkie	*Reader in Mathematical Logic, University of Oxford*

This publication forms part of an Open University course. Details of this and other Open University courses can be obtained from the Student Registration and Enquiry Service, The Open University, PO Box 197, Milton Keynes, MK7 6BJ, United Kingdom: tel. +44 (0)870 300 6090, e-mail general-enquiries@open.ac.uk

Alternatively, you may visit the Open University website at http://www.open.ac.uk where you can learn more about the wide range of courses and packs offered at all levels by The Open University.

To purchase a selection of Open University course materials, visit http://www.ouw.co.uk, or contact Open University Worldwide, Michael Young Building, Walton Hall, Milton Keynes, MK7 6AA, United Kingdom, for a brochure: tel. +44 (0)1908 858793, fax +44 (0)1908 858787, e-mail ouw-customer-services@open.ac.uk

The Open University, Walton Hall, Milton Keynes, MK7 6AA.

First published 1996. Reprinted 2001 and 2003. New edition 2007 with corrections.

Copyright © 1996 The Open University

All rights reserved; no part of this publication may be reproduced, stored in a retrieval system, transmitted or utilised in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without written permission from the publisher or a licence from the Copyright Licensing Agency Ltd. Details of such licences (for reprographic reproduction) may be obtained from the Copyright Licensing Agency Ltd, Saffron House, 6–10 Kirby Street, London EC1N 8TS; website http://www.cla.co.uk.

Open University course materials may also be made available in electronic formats for use by students of the University. All rights, including copyright and related rights and database rights, in electronic course materials and their contents are owned by or licensed to The Open University, or otherwise used by The Open University as permitted by applicable law.

In using electronic course materials and their contents you agree that your use will be solely for the purposes of following an Open University course of study or otherwise as licensed by The Open University or its assigns.

Except as permitted above you undertake not to copy, store in any medium (including electronic storage or use in a website), distribute, transmit or re-transmit, broadcast, modify or show in public such electronic materials in whole or in part without the prior written consent of The Open University or in accordance with the Copyright, Designs and Patents Act 1988.

Edited, designed and typeset by The Open University, using the Open University TEX System.

Printed and bound in the United Kingdom by Charlesworth Press, Wakefield.

ISBN 978 0 7492 2268 0

2.1

CONTENTS

Introduction 4

1 The Primes 5
- 1.1 Basic properties 5
- 1.2 The Sieve of Eratosthenes 7
- 1.3 The Fundamental Theorem of Arithmetic 8

2 The Prime Decomposition of Integers 11
- 2.1 The prime decomposition of divisors 11
- 2.2 The τ function 13

3 The Infinitude of the Primes 14
- 3.1 Euclid's Theorem 14
- 3.2 Primes in arithmetic progression 16
- 3.3 Primes generated by polynomials 20

4 Famous Problems Concerning Primes 22
- 4.1 Proximity of primes 22
- 4.2 The Goldbach Conjecture 24
- 4.3 The Prime Number Theorem 25

5 Fibonacci Numbers 27
- 5.1 The Fibonacci sequence 27
- 5.2 Properties of Fibonacci numbers 29

Additional Exercises 33

Solutions to the Problems 35

Solutions to Additional Exercises 39

Appendix: Table of Primes 46

Index 48

INTRODUCTION

The fact that some numbers break up into divisors, like $12 = 3 \times 4$, whereas others, like 13, cannot be broken up must surely have intrigued most people at some stage of their mathematical education. The numbers which cannot be broken up

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ 41,\ 43,\ \ldots$$

are called the *primes*, and we shall rapidly discover that they form a central concept in any study of the theory of numbers. Almost every investigation involves them in one way or another.

As numbers get larger the likelihood of having divisors would appear to increase, suggesting that there is a limit beyond which numbers cannot be prime. What is the largest prime? How many primes are there? In Book IX of *Elements,* Euclid answered both these questions by showing that, on the contrary, the sequence of primes does not end; there are infinitely many primes. Euclid's proof of this fact, which we shall reproduce in this unit, has universal appeal because of its elegance and simplicity.

Since Euclid, a prodigious amount of effort has been expended on producing more extensive tables of prime numbers and the search to find larger and larger primes has continued unabated. The first significant record of a table of primes is due to Fibonacci who, in the year 1202, listed primes up to 100. By 1603 Pietro Cataldi had listed all primes up to 750. Developments followed closely after that and by the end of the 18th century lists of all primes up to one million were recorded. The arrival of electronic computers accelerated discoveries to such an extent that it is difficult to keep track of the largest known prime. By the 1990's numbers such as $2^{756\,839} - 1$, which when written out has a mere 227 832 digits, had been proved by computer to be prime.

How would we go about producing a list of all primes up to, say, 1000? A simple-minded approach would be to take each integer in turn and check its divisibility by each smaller positive integer, concluding that the number is prime if none of the smaller positive integers (other than 1) divides it. However, the amount of calculation involved in this approach makes it impractical, even with the benefit of a number of short-cuts which are available. An early Greek mathematician, Eratosthenes (276–194 BC), devised a superior approach which we shall meet, and use, in this unit.

Since the dawn of mathematical history, problems involving primes and how to classify them have fascinated and attracted the attention of the greatest mathematical minds. How many primes p are there for which $p + 2$ is also prime? Can every even integer from 4 onwards be written as the sum of two primes? What is the maximum length for a sequence of consecutive integers none of which is prime? Throughout this unit we shall be looking at classical problems, including these, providing answers to some and discussing others which, despite considerable numerical evidence in support of their validity, remain unsolved in spite of numerous attempts at proofs over the years.

How is this infinite set of primes distributed amongst the set of all integers? Could, for example, every sixth integer from 5 onwards be prime? This arithmetic progression begins

$$5,\ 11,\ 17,\ 23,\ 29,\ \ldots;$$

the first five members of this sequence are prime but the next, 35, is not. Can any arithmetic progression consist of primes alone? Can an arithmetic progression contain infinitely many primes? We shall look at some problems in this area, providing answers to questions concerning the presence of primes first in arithmetic progressions, and then in other sequences.

In the final section of the unit we introduce and discuss another intriguing sequence of integers about which many questions can be answered: the *Fibonacci sequence.* As well as being of interest for its own sake, the Fibonacci sequence will enable us to gain practice in applying results and techniques developed elsewhere in the first two units, in particular those concerning divisibility properties.

1 THE PRIMES

1.1 Basic properties

We begin with the key definition.

Definition 1.1 Prime numbers

An integer n, where $n \geq 2$, is said to be *prime* if it has no positive divisor other than itself and 1. Otherwise n is said to be *composite.*

In future, for brevity, we shall often replace phrases such as 'integer n, where $n \geq 2$' by 'integer $n \geq 2$'.

Notice that we have excluded consideration of 0 and the negative integers from these definitions; we shall not be concerned with the primality or otherwise of non-positive integers. Notice also that the integer 1 is classified neither as prime nor as composite. As the composite integers are essentially those which can be broken down into products of at least two non-trivial (i.e. not itself and 1) positive divisors, it is natural to exclude 1 from the composite integers. On the other hand we do not want to list 1 amongst the primes for a variety of reasons. For example, if 1 were to be considered as a prime,

$$6 = 2 \times 3 = 1 \times 2 \times 3 = 1 \times 1 \times 2 \times 3$$

would be three (of infinitely many) different ways of expressing 6 as a product of primes. Excluding 1 from the list of primes enables us to express any integer greater than or equal to 2 as a *unique* product of primes. This result, which we shall prove shortly, is of great importance in the study of number theory.

By a product we mean any number of integers multiplied together including the possibility of a single integer on its own, such as 2 here.

Is 211 prime or is it composite? If we can spot an integer in the range 2 to 210 which divides 211 we can conclude immediately that 211 is composite. On the other hand, to show that 211 is prime there are a lot of potential divisors to be eliminated. Do we have to test division by all the numbers in the range 2 to 210? Fortunately we do not. The following two results show that the list of potential divisors can be drastically reduced. The first of these results appeared in Book VII of *Elements.*

Theorem 1.1

Each integer $n \geq 2$ is divisible by some prime number.

If n is prime then n is a prime divisor of itself.

Proof of Theorem 1.1

Preparing for a proof by Mathematical Induction (using the Second Principle), let $P(n)$ be the statement that the integer $n \geq 2$ is divisible by some prime number.

The statement $P(2)$ is certainly true, since 2 divides 2 and 2 is prime, and this provides the basis for the induction.

For the induction step suppose that for some integer $k \geq 2$, each of $P(2), P(3), \ldots, P(k)$ is true; that is, suppose that each of the integers $2, 3, \ldots, k$ is divisible by some prime. Now consider the next integer, $k+1$. Either $k+1$ is prime or it is composite. If it is a prime it is divisible by the prime $k+1$ itself. If it is composite, then $k+1 = rs$, where r and s are integers with $2 \leq r \leq k$, whereupon the induction hypothesis tells us that there is some prime p which divides r. But then p divides r and r divides $k+1$ and so p divides $k+1$. In either case we conclude that $k+1$ is divisible by some prime, confirming the truth of $P(k+1)$.

The result follows by Mathematical Induction. ■

The next result determines a limit to the number of divisions one has to make in order to decide whether a given integer $n \geq 2$ is prime or not.

Theorem 1.2

If the integer $n \geq 2$ is composite, then it is divisible by some prime $p \leq \sqrt{n}$.

Proof of Theorem 1.2

As n is composite we can write $n = ab$, where a and b are integers with $2 \leq a \leq b$. Now we cannot have $a > \sqrt{n}$, for that would imply $b > \sqrt{n}$ and the product ab would exceed n. So $a \leq \sqrt{n}$. At this point we can invoke Theorem 1.1 which guarantees the existence of a prime p dividing a (and therefore dividing n). As $p \leq a \leq \sqrt{n}$, p suffices as the required prime. ■

The prime numbers which are less than $\sqrt{211}$ are 2, 3, 5, 7, 11 and 13, and so if 211 is composite it must be divisible by one of these primes. However, straightforward division shows that this is not the case. 211 has remainder 1 when divided by each of 2, 3, 5 and 7, remainder 2 on division by 11 and remainder 3 on division by 13. Hence 211 is prime.

Problem 1.1

Which, if any, of the integers 111, 113, 115 and 117 is prime?

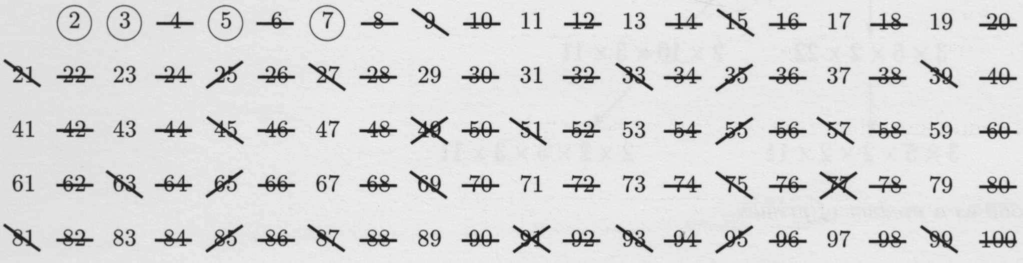
Problem 1.2

To test whether or not 499 is a prime, for which numbers is it sufficient to check divisibility?

The problem of how to find the primes up to a given integer is tackled in the next section.

1.2 The Sieve of Eratosthenes

Eratosthenes devised a relatively simple way of listing all the primes up to some number. The method is illustrated for primes up to 100 in Figure 1.1. It works as follows. Write down in order all the positive integers from 2 up to the chosen limit, 100 in this case. The first number 2 is prime, so we ring it, and then cross out every second number after 2 in the list. These are the non-trivial multiples of 2 (and therefore composite) and are shown crossed out with a horizontal bar in the figure. Having completed this task we return to the number 2. The first number following 2 which is not crossed out is 3 so we ring it as being prime and proceed to cross out (with a \) every third number following 3, if not already crossed out. Returning to 3, the first number after 3 which is not crossed out is 5, so we ring it as being prime and cross out (with a /) every fifth number after it, if not already crossed out. Continuing in this way, 7 is ringed next and every seventh number after it is crossed out (with a X).

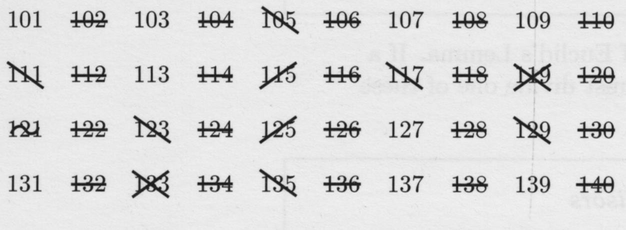


② ③ 4 ⑤ 6 ⑦ 8 9 10 11 12 13 14 15 16 17 18 19 20
21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40
41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60
61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80
81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100

Figure 1.1 Sieving the primes up to 100

The next uncrossed number is the prime 11, but as 11 exceeds $\sqrt{100}$ it turns out that we are finished. All multiples of 11, and, with the same reasoning, multiples of larger primes, must already have been crossed out because any number in the range 2 to 100 which is divisible by 11 is, by Theorem 1.2, also divisible by a prime less than $\sqrt{100}$, and so is a multiple of one of the already ringed primes. We can therefore now ring all the uncrossed numbers in the knowledge that they complete the primes up to 100.

To extend the list of primes beyond 100 we do not have to begin the sieve again. For instance, to pick up the primes in the range 101 to 140 we know that it is a matter of crossing out from a list of these 40 numbers the multiples of each of the primes up to $\sqrt{140}$; that is, we cross out the first multiple of 2, namely 102, and every second number, then the first multiple of 3 (also 102) and every third number, and similarly for primes 5, 7 and 11. Figure 1.2 shows the extension with the one occurring multiple of 11 crossed out (with a $\sim$). The numbers not crossed out are the primes.



101 102 103 104 105 106 107 108 109 110
111 112 113 114 115 116 117 118 119 120
121 122 123 124 125 126 127 128 129 130
131 132 133 134 135 136 137 138 139 140

Figure 1.2 Sieving the primes in the range 101 to 140

Problem 1.3

Extend the sieve to find all primes up to 200.

1.3 The Fundamental Theorem of Arithmetic

Given any composite integer, it can be expressed, possibly in many ways, as a product of divisors. For instance, observing that 11 divides 660 we may express the latter as 11 × 60. Now the divisor 60 is composite, so it may be broken down further into, for example, 4 × 15, so that $660 = 11 \times 4 \times 15$. The divisors 4 and 15 are each composite, so they can be broken down further. Indeed, by continuing to break down any composite divisor in this way, we can eventually express the original number as a product of primes. Figure 1.3 shows three ways in which 660 can be broken down to its prime divisors.

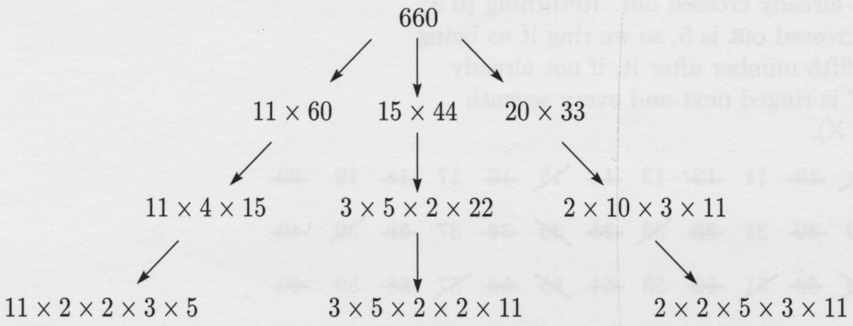


Figure 1.3   Expressing 660 as a product of primes

What is noticeable is that in all these ways of breaking down 660 we end up with the same product of primes; the order in which they are written varies, but in all cases $660 = 2 \times 2 \times 3 \times 5 \times 11$. Our next goal is to show that every integer greater than 1 is expressible as a product of primes in a unique way (except for the order in which the primes are written). But on the way we shall need some divisibility properties involving primes.

First we record one simple property, concerning greatest common divisors, which will come up frequently. Suppose that p is prime and n is any integer. What can we say about $\gcd(n, p)$? As the only divisors of prime p are p itself and 1, $\gcd(n, p)$ has just the two possible values, namely p and 1. Now $\gcd(n, p) = p$ precisely when p divides n. Hence:

The value of gcd(n, p)

If p is a prime and n is any integer, then

$$\gcd(n,p) = \begin{cases} p, & \text{if } p \text{ divides } n, \\ 1, & \text{otherwise.} \end{cases}$$

Theorem 1.3, which follows, is a consequence of Euclid's Lemma. If a prime p divides a product of numbers then it must divide one of these numbers.

Theorem 1.3 Euclid's Lemma for prime divisors

If p is prime and p divides the product $a_1 a_2 \ldots a_n$ then p divides a_i, for some integer i, where $1 \leq i \leq n$.

Proof Theorem 1.3

We prove the result by Mathematical Induction on the number of terms in the product. With that goal in mind let $P(n)$ be the statement of the theorem.

We have the basis for induction since $P(1)$ is trivially true, for it states that if p divides a_1, then p divides a_1.

Heading for the induction step, suppose that $P(k)$ is true for some integer $k \geq 1$, that is, if p divides the product of any k integers then p divides one of them. Now consider any product of $k+1$ integers which is divisible by p, say

$$p \mid a_1 a_2 \ldots a_k a_{k+1}.$$

Either p divides a_{k+1} or it does not. If p divides a_{k+1} we are finished. If p does not divide a_{k+1} then $\gcd(p, a_{k+1}) = 1$. Since p divides the product $(a_1 a_2 \ldots a_k)a_{k+1}$ and $\gcd(p, a_{k+1}) = 1$ we conclude, by Euclid's Lemma, that p divides $a_1 a_2 \ldots a_k$. But then, by the induction hypothesis, p divides a_i for some i, where $1 \leq i \leq k$.

Putting the two possibilities together, either p divides a_{k+1} or p divides a_i for some i, where $1 \leq i \leq k$, which verifies that $P(k+1)$ is true. This completes the proof. ■

One consequence of Theorem 1.3 merits recording:

Corollary to Euclid's Lemma

If p, p_1, p_2, ..., p_n are primes such that

$$p \mid p_1 p_2 \ldots p_n,$$

then $p = p_i$ for some i, where $1 \leq i \leq n$.

Proof of the Corollary

Theorem 1.3 tells us that p divides p_i for some i, where $1 \leq i \leq n$. But the only divisors of p_i are 1 and p_i, and as 1 is not a prime, it follows that $p = p_i$. ■

The following example makes use of these results.

Example 1.1

Let p be prime and a and b be integers. Show that:

(a) if p divides a^n, then p^n divides a^n;

(b) if $\gcd(a, b) = p$, then $\gcd(a^n, b^n) = p^n$.

(a) Using Theorem 1.3 with $a_1 = a_2 = \cdots = a_n = a$, we deduce immediately that if p divides a^n then p divides a. Hence $a = pr$, for some integer r. Raising both sides of this equation to the power n gives $a^n = p^n r^n$, which tells us that p^n divides a^n.

(b) If $\gcd(a, b) = p$, there exist integers r and s such that $a = pr$ and $b = ps$, with $\gcd(r, s) = 1$. But then

$$\begin{aligned} \gcd(a^n, b^n) &= \gcd(p^n r^n, p^n s^n) \\ &= p^n \gcd(r^n, s^n), \quad \text{by Problem 4.4 (d) of } \textit{Unit 1}. \end{aligned}$$

When proving results involving two integers, it is sometimes useful, as here, to divide each by their gcd and then work with the resulting integers which are relatively prime by Theorem 4.5 of *Unit 1*.

It remains to show that $\gcd(r^n, s^n) = 1$.

Suppose q is a prime which divides $\gcd(r^n, s^n)$. Then q divides r^n and q divides s^n. As we saw in part (a) this implies that q divides r and q divides s, so that q divides $\gcd(r, s)$. But $\gcd(r, s) = 1$, contradicting the existence of such a prime q.

Hence $\gcd(r^n, s^n) = 1$, which completes the proof. ◆

We are just about ready for our main result of this section, but first a word about notation. We have just seen several ways of expressing 660 as a product of primes, the only difference between the expressions being the order in which the primes were written. Conventionally, when writing a number down as a product of its prime divisors, we shall arrange the primes in ascending order with like primes collected together as a power. For instance we shall write 660 as

$$660 = 2^2 \times 3 \times 5 \times 11.$$

This convention removes the ambiguity of ordering and, as we are about to see, renders a unique representation of the integer as a product of its prime divisors. We refer to this as the *prime decomposition* of the integer.

Problem 1.4

Give the prime decompositions of each of the integers 168, 226 and 36 000.

Theorem 1.4 The Fundamental Theorem of Arithmetic

Any integer $n \geq 2$ can be written uniquely in the form

$$n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r},$$

where p_i, $i = 1, \dots, r$, are primes with $p_1 < p_2 < \dots < p_r$ and each k_i, $i = 1, \dots, r$, is a positive integer.

As its name suggests, this theorem is central to many investigations in number theory.

Proof of Theorem 1.4

We prove the theorem in two parts. First, we show the *existence* of such a decomposition, that is, we show that n can be expressed as such a product of primes. Second, we show that the prime decomposition obtained is *unique*.

Existence

With proof by Mathematical Induction in mind, let $P(n)$ be the proposition that n can be expressed as a product of primes. We require to show that $P(n)$ is true for all $n \geq 2$.

Now $P(2)$ is certainly true, since 2 is a prime, so we have the basis for the induction.

Suppose that, for some integer $k \geq 2$, $P(2)$, $P(3)$, …, $P(k)$ are all true. That is, each of 2, 3, …, k can be written as a product of primes. Now consider the integer $k+1$. By Theorem 1.1, $k+1$ is divisible by some prime p and so we may write $k+1 = pr$, for some integer r. If $r = 1$, $k+1$ is a prime and we are done. If $r > 1$ then, as $r < k+1$, the induction hypothesis tells us that r is a product of primes, whereupon $k+1 = pr$ is also a product of primes. It follows therefore that $P(k+1)$ is true.

Hence, by the Second Principle of Mathematical Induction, $P(n)$ is true for all integers $n \geq 2$.

Uniqueness

Suppose that some integer $n \geq 2$ has two representations as a product of primes, say,

$$\begin{aligned} n &= p_1 p_2 \dots p_r, \quad \text{where } p_1 \leq p_2 \leq \dots \leq p_r, \\ &= q_1 q_2 \dots q_s, \quad \text{where } q_1 \leq q_2 \leq \dots \leq q_s. \end{aligned}$$

In these expressions for n we have kept the primes separate rather than collecting them in powers.

Now p_1 divides n and so p_1 divides the product $q_1 q_2 \dots q_s$. By the Corollary to Euclid's Lemma, this gives $p_1 = q_j$ for some $1 \leq j \leq s$. As $q_1 \leq q_j$ we conclude that $q_1 \leq p_1$. But there is symmetry between the p's and q's. So similarly we argue that since q_1 divides n, we have $q_1 = p_i$ for some $1 \leq i \leq r$, which leads to $p_1 \leq q_1$. Combining the two inequalities gives $p_1 = q_1$.

Since p_1 divides n we have $n = p_1 n_1$ for some integer n_1. Hence

$$n_1 = p_2 \dots p_r = q_2 \dots q_s,$$

and a repetition of the argument gives $p_2 = q_2$. Then, putting $n = p_1 p_2 n_2$, we get

$$n_2 = p_3 \dots p_r = q_3 \dots q_s,$$

giving $p_3 = q_3$.

We can continue in this way cancelling equal primes from the left of the two products.

If $r < s$ then we obtain $p_i = q_i$ for $1 \le i \le r$ and we are left with

$$1 = q_{r+1} \dots q_s.$$

This is a contradiction, since the q_i are primes. The assumption that $r > s$ leads to a similar contradiction. Hence $r = s$ and the proof of the uniqueness of the prime decomposition is complete. ■

Problem 1.5

Show that the integer $n > 1$ with prime decomposition $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ is a square if, and only if, each of the exponents k_i is even.

Problem 1.6

Use the identity $n^3 - 1 = (n-1)\left(n^2 + n + 1\right)$ to prove that the only prime of the form $n^3 - 1$ is 7.

2 THE PRIME DECOMPOSITION OF INTEGERS

2.1 The prime decomposition of divisors

When the prime decomposition of an integer is given, it is a simple matter to obtain all its divisors.

Remember that we only consider *positive* divisors.

Problem 2.1

Given that $252 = 2^2 \times 3^2 \times 7$, write down as many divisors as you can find of 252, expressing each one in its prime decomposition. Can you formulate a conjecture about the set of all divisors of 252?

One of the divisors of 252 is 1, which does not have a prime decomposition. For convenience we shall define the prime decomposition of 1 to be 1 itself.

The observations in the solution to Problem 2.1 lead to the following generalization.

Theorem 2.1 Divisors of an integer

Let n be an integer greater than 1, with prime decomposition

$$n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}.$$

Then the set of all divisors of n is the set of integers

$$\left\{p_1^{h_1} p_2^{h_2} \dots p_r^{h_r} : 0 \le h_i \le k_i \text{ for } i = 1, 2, \dots, r\right\}$$

Proof of Theorem 2.1

Certainly each integer in the given set is a divisor of n because $k_i - h_i \ge 0$ for each i and

$$n = \left(p_1^{h_1} p_2^{h_2} \dots p_r^{h_r}\right) p_1^{k_1 - h_1} p_2^{k_2 - h_2} \dots p_r^{k_r - h_r}.$$

Our task now is to show that the integers in the given set, which are distinct by the uniqueness of prime decomposition, are the *only* divisors of n. To that end, let $d > 1$ be a divisor of n and let p be a prime divisor of d. Since p divides d and d divides n we know that p divides n. Therefore, by the Corollary to Euclid's Lemma, $p = p_i$ for some i, where $1 \leq i \leq r$. It follows therefore that the only primes dividing d come from the set $\{p_i : 1 \leq i \leq r\}$. Hence we can write $d = p_1^{h_1} p_2^{h_2} \dots p_r^{h_r}$, where each h_i is a non-negative integer.

Finally, to show $h_i \leq k_i$ we utilize the fact that d divides n and that, as a consequence, $p_i^{h_i}$ divides n. As $p_1, p_2, \dots, p_r$ are distinct primes, the Corollary to Euclid's Lemma confirms that p_1 does not divide $p_2^{k_2} p_3^{k_3} \dots p_r^{k_r}$. Hence $\gcd\left(p_1^{h_1}, p_2^{k_2} p_3^{k_3} \dots p_r^{k_r}\right) = 1$ and, coupled with the fact that $p_1^{h_1}$ divides $n = p_1^{k_1}\left(p_2^{k_2} p_3^{k_3} \dots p_r^{k_r}\right)$, Euclid's Lemma show that $p_1^{h_1}$ divides $p_1^{k_1}$, the latter amounting to $h_1 \leq k_1$. The same argument shows that $h_2 \leq k_2, \dots, h_r \leq k_r$. ■

Problem 2.2

Let $m = 3^3 \times 5 \times 17^2$ and $n = 2 \times 3^2 \times 7 \times 17^4$.

(a) How many (positive) divisors does m have? How many does n have?

(b) List the common divisors of m and n.

(c) Determine the prime decompositions of $\gcd(m, n)$ and of $\operatorname{lcm}(m, n)$.

Let us look generally at the problem of determining $\gcd(m, n)$ and $\operatorname{lcm}(m, n)$ when the prime decompositions of m and n are at hand. We may suppose that

$$m = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} \quad \text{and} \quad n = p_1^{l_1} p_2^{l_2} \dots p_r^{l_r},$$

where $p_1, p_2, \dots, p_r$ are the primes which divide either m or n. This means that what we have written here are not necessarily the prime decompositions; to get the same primes listed for both m and n it may be necessary to include some with exponent 0. For example, $k_i = 0$ if p_i divides n but p_i does not divide m.

A divisor of m is an integer

$$d = p_1^{h_1} p_2^{h_2} \dots p_r^{h_r},$$

where $0 \leq h_i \leq k_i$ for each $i = 1, 2, \dots, r$. Also, d divides n if, and only if, $h_i \leq l_i$ for each $i = 1, 2, \dots, r$. Combining these two conditions: d is a common divisor of m and n if, and only if, $0 \leq h_i \leq \min\{k_i, l_i\}$ for each $i = 1, 2, \dots, r$. For its greatest value d requires the largest possible exponent for each of its primes, and therefore

If a and b are integers, then $\min\{a, b\}$ denotes the smaller of a and b.

Prime decomposition of gcd(m, n)

$$\gcd(m, n) = p_1^{\min\{k_1, l_1\}} p_2^{\min\{k_2, l_2\}} \dots p_r^{\min\{k_r, l_r\}}.$$

In words, the largest prime powers dividing $\gcd(m, n)$ are obtained by raising each prime which divides either m or n to the power which is the smaller of its exponents in m and n. To write $\gcd(m, n)$ in prime decomposition, each resulting term $p_i^{\min\{k_i, l_i\}}$ in which the exponent $\min\{k_i, l_i\}$ is 0 is removed from the expression. If $\min\{k_i, l_i\} = 0$ for each $i = 1, 2, \dots, r$, then $\gcd(m, n) = 1$.

A corresponding result for lcm(m, n) is readily obtained from the formula relating lcm(m, n) to gcd(m, n):

$$\begin{aligned}\operatorname{lcm}(m,n) = \frac{mn}{\gcd(m,n)} &= \frac{\left(p_1^{k_1}\dots p_r^{k_r}\right)\left(p_1^{l_1}\dots p_r^{l_r}\right)}{p_1^{\min\{k_1,l_1\}}\dots p_r^{\min\{k_r,l_r\}}}\\ &= p_1^{k_1+l_1-\min\{k_1,l_1\}}\dots p_r^{k_r+l_r-\min\{k_r,l_r\}}.\end{aligned}$$

Now for any two integers k and l,

$$k + l - \min\{k, l\} = \max\{k, l\}.$$

This follows since $\min\{k, l\}$ is the smaller of k and l and subtracting the smaller of k and l from $k + l$ leaves the larger. Therefore we have the following result.

If a and b are integers, then $\max\{a, b\}$ denotes the larger of a and b.

Prime decomposition of lcm(m, n)

$$\operatorname{lcm}(m,n) = p_1^{\max\{k_1,l_1\}}p_2^{\max\{k_2,l_2\}}\dots p_r^{\max\{k_r,l_r\}}$$

In words, the prime decomposition of lcm(m, n) is obtained by raising each prime which divides either m or n to the larger of its exponents in m and n.

Problem 2.3

If $m = 3^3 \times 5^3 \times 11 \times 19$ and $n = 2 \times 3^2 \times 7 \times 11$ write down the prime decompositions of gcd(m, n) and lcm(m, n).

Diversion

The sequence of palindromic primes.

2, 3, 5, 7, 11, 101, 131, 151, 181, 191, 313,
…, 929, 10301, 10501, 10601, 11311,
…, 98389, 98689, 1003001, 1008001, …

2.2 The τ function

From the prime decomposition of an integer n, Theorem 2.1 demonstrates how to list the divisors of n. As a consequence, this theorem tells us exactly how many divisors the integer n has. The number of (positive) divisors of an integer is used to define a function, denoted by the Greek letter τ.

τ is the Greek letter tau, usually pronounced either to rhyme with 'saw' or to rhyme with 'how'.

Definition 2.1 The τ function

For any integer $n \geq 1$, $\tau(n)$ is defined to be the number of distinct divisors of n, including 1 and n.

Notice that $\tau(1) = 1$.

To determine the value of $\tau(n)$ from the prime decomposition of n involves little more than some elementary arithmetic.

Theorem 2.2 The formula for $\tau(n)$

For any integer $n \geq 2$, with prime decomposition

$$n = p_1^{k_1}p_2^{k_2}\dots p_r^{k_r},$$

we have

$$\tau(n) = (k_1 + 1)(k_2 + 1)\cdots(k_r + 1).$$

Proof of Theorem 2.2

We have established that any divisor d of $p_1^{k_1}p_2^{k_2}\dots p_r^{k_r}$ has prime decomposition $p_1^{l_1}p_2^{l_2}\dots p_r^{l_r}$, where $0 \le l_i \le k_i$ for each $i = 1, 2, \dots, r$. There are k_1+1 choices for l_1, k_2+1 choices for $l_2, \dots$ and k_r+1 choices for l_r. This makes $(k_1+1)(k_2+1)\dots(k_r+1)$ choices in all, and, because of the uniqueness of prime decomposition, each of these choices results in a distinct divisor.

■

Example 2.1

Find all integers less than 100 which have exactly 10 divisors.

If $\tau(n) = 10$, then $(k_1+1)(k_2+1)\dots(k_r+1) = 10$, where the positive integers k_i are the exponents in the prime decomposition of n. There are only two ways that 10 can be expressed as the product of integers greater than 1, namely as 2×5 or as 10. In the former case $k_1 = 1$ and $k_2 = 4$ giving $n = p_1p_2^4$, and in the latter case $k_1 = 9$, giving $n = p_1^9$.

Notice that in writing $n = p_1p_2^4$ here, we do not know that $p_1 < p_2$, so the order of the primes is not necessarily as it should be in the prime decomposition. In answering questions like this we shall be lax about writing primes in ascending order.

There are two numbers of the form $p_1p_2^4$ which do not exceed 100, namely $3 \times 2^4 = 48$ and $5 \times 2^4 = 80$. The smallest number of the form p_1^9 is $2^9 = 512$, so all numbers of this form exceed 100. Hence the only possibilities are 48 and 80.

♦

Problem 2.4

Find the smallest integer which has exactly 24 divisors.

---

3 THE INFINITUDE OF THE PRIMES

3.1 Euclid's Theorem

In Book IX of *Elements*, Euclid produced a simple but elegant proof of the existence of infinitely many primes. The essence of Euclid's proof comes from consideration of the sequence of numbers $\{P_n\}$, $n \ge 1$, where P_n is obtained by adding 1 to the product of the first n primes:

$$\begin{aligned}
P_1 &= 2 + 1 = 3\\
P_2 &= 2 \times 3 + 1 = 7\\
P_3 &= 2 \times 3 \times 5 + 1 = 31\\
P_4 &= 2 \times 3 \times 5 \times 7 + 1 = 211\\
P_5 &= 2 \times 3 \times 5 \times 7 \times 11 + 1 = 2311\\
&\vdots
\end{aligned}$$

It is interesting to note that the first five numbers in this sequence are prime. However, at this point the coincidence ceases as the next number $P_6 = 30\,031 = 59 \times 509$ is composite, as also are P_7, P_8, P_9 and P_{10}. The next number, P_{11} is prime, but then all the subsequent P_n are composite until P_{75}. At the time of writing this unit it is not known whether infinitely many numbers in the sequence $\{P_n\}$ are prime, nor indeed whether infinitely many numbers in this sequence are composite, though at least one of these must be true!

$P_{75} = 2 \times 3 \times 5 \times \dots \times 379 + 1.$

The crucial point concerning the numbers in this sequence is illustrated as follows for the particular term

$$P_5 = 2 \times 3 \times 5 \times 7 \times 11 + 1.$$

Now P_5 is of the form $2r + 1$ and so it has remainder 1 on dividing by 2. Similarly P_5 is of the form $3s + 1$ and so has remainder 1 on dividing by 3. In just the same way P_5 has remainder 1 on dividing by each of the primes 5, 7 and 11. In summary, P_5 has been constructed so that it is not divisible by any of the first five primes, 2, 3, 5, 7 or 11. Now we know, by Theorem 1.1, that P_5 is divisible by some prime and so P_5 'uncovers' a sixth prime; either P_5 is itself prime, or it is divisible by a prime which is not one of the primes 2, 3, 5, 7 or 11 from which it has been constructed.

The same argument applies to each of the numbers

$$P_n = p_1 p_2 p_3 \ldots p_n + 1.$$

Now P_n is not divisible by any of the primes $p_1, p_2, p_3, \ldots, p_n$ as it has remainder 1 on dividing by each of them. So P_n is divisible by some 'new' prime.

It follows that there cannot be just a finite number of primes because from such a finite list we can always construct one more.

Let us present this argument formally:

Theorem 3.1 Euclid's Theorem

There are infinitely many primes.

Proof of Euclid's Theorem.

The proof is by contradiction.

Suppose the theorem is not true and that there are only finitely many primes, $p_1, p_2, p_3, \ldots, p_n$. Consider the number

$$N = p_1 p_2 p_3 \ldots p_n + 1.$$

Since N is divisible by some prime, and as $p_1, p_2, p_3, \ldots, p_n$ are presumed to be the only primes, N is divisible by one of the primes p_i in this list. But then, as p_i divides N and p_i divides $p_1 p_2 \ldots p_i \ldots p_n$, we have that p_i divides the integer combination $N - p_1 p_2 \ldots p_i \ldots p_n$; that is p_i divides 1. As $p_i \geq 2$ this is a contradiction.

Therefore the supposition that there are only finitely many primes must be false and hence there are infinitely many primes. ■

Euclid's argument can be applied to give an upper bound on the size of the nth prime. Adopting the notation that p_n is the nth prime number we see that

$$p_{n+1} \leq p_1 p_2 p_3 \ldots p_n + 1$$

and so

$$p_{n+1} < p_n^n + 1.$$

This, however, is not a very useful bound because, for instance, taking $n = 7$ it only tells us that the 8th prime, namely 19, does not exceed $17^7 + 1 \simeq 4.1 \times 10^8$.

Example 3.1 finds an alternative upper bound.

Example 3.1

Show that the nth prime p_n satisfies the inequality $p_n \leq 2^{2^{n-1}}$.

Heading towards a proof by the Second Principle of Mathematical Induction, let the statement to be proved be $P(n)$.

The result is true for $n = 1$, since $P(1)$ states that $2 \leq 2^{2^0} = 2$. This gives the basis for the induction.

We now assume that, for some integer $k \geq 1$, $P(1), P(2), \ldots, P(k)$ are all true. To complete the induction step we must show that $P(k+1)$ is true; that is, $p_{k+1} \leq 2^{2^k}$.

$$\begin{aligned} p_{k+1} &\leq p_1 p_2 p_3 \ldots p_k + 1, \quad \text{by Euclid's argument,} \\ &\leq 2 \times 2^2 \times 2^{2^2} \times \cdots \times 2^{2^{k-1}} + 1, \quad \text{by the induction hypothesis,} \\ &\leq 2^{1+2+2^2+2^3 \ldots + 2^{k-1}} + 1, \quad \text{by the law of indices,} \\ &\leq 2^{2^k - 1} + 1, \quad \text{by the sum of a geometric progression,} \\ &\leq 2^{2^k-1} + 2^{2^k-1} = 2^{2^k}, \quad \text{since } 1 \leq 2^{2^k-1} \text{ for all } k. \end{aligned}$$

This completes the proof. ◆

The upper bound for the nth prime given in Example 3.1 is actually even more extravagant than our previous one. It tells us that the 8th prime now does not exceed $2^{2^7} = 2^{128} \simeq 3.4 \times 10^{38}$. You will be pleased to hear that much better bounds are known.

In 1841, the French mathematician, Bertrand, posed an interesting conjecture concerning the location of primes.

Bertrand's Conjecture

For each integer $n \geq 2$, there exists a prime p such that $n < p < 2n$.

The proof of Bertrand's Conjecture is outside the scope of this course.

Bertrand checked his conjecture for all n up to three million which, though not quite the daunting task it might at first sound, was nevertheless quite an achievement at that time.

A proof was given nine years later, in 1850, by the Russian mathematician Tchebychef. In fact Tchebychef improved on Bertrand's result by showing that, except for a finite number of values of n, there is always a prime between n and $\frac{6}{5}n$. In fact there is nothing special about Tchebychef's multiplier $\frac{6}{5}$. It is now known that, for any positive number ε, from some integer N onwards there is always a prime number between n and $(1+\varepsilon)n$. As you would expect, the smaller the ε is, the larger the N becomes.

Problem 3.1

Assuming Bertrand's Conjecture, prove that the nth prime p_n satisfies the inequality $p_n < 2^n$, for all integers $n \geq 2$.

3.2 Primes in arithmetic progression

Having seen that there are infinitely many primes, it is natural to ask how these primes are distributed amongst the set of integers. As we shall discover, interesting questions in this area are plentiful, but answers to them are not so readily at hand. One area in which we can provide some answers concerns the occurrences of primes in arithmetic progressions. For instance, consider the progression

$$3,\ 7,\ 11,\ 15,\ 19,\ \ldots,\ 4k+3, \ldots.$$

We see that both primes and composites are occurring, and we can ask whether infinitely many members of the sequence are prime. With an eye on Euclid's proof above we can, with a little care, produce an argument on the same lines to prove that infinitely many of these numbers are prime.

Consider the following sequence of numbers.

$$\begin{aligned}Q_1 &= 4 \times (3) - 1 = 11\\ Q_2 &= 4 \times (3 \times 7) - 1 = 83\\ Q_3 &= 4 \times (3 \times 7 \times 11) - 1 = 923\\ Q_4 &= 4 \times (3 \times 7 \times 11 \times 19) - 1 = 17\,555\\ &\vdots\end{aligned}$$

In general, the number Q_n is obtained by multiplying together the first n primes in the arithmetic progression, (note that composites such as 15 are excluded) then multiplying by 4 and finally subtracting 1. The reason for multiplying by 4 and subtracting 1 is to ensure that Q_n is itself of the form $4k+3$. The interesting outcome of this is that Q_n turns out to be divisible by a prime of type $4k+3$ which is larger than any of the n primes involved in its construction. Of the listed values 11 and 83 are primes of the form $4k+3$ while

Note that any number of the form $4q-1$ is also of the form $4k+3$ since $4q-1 = 4(q-1)+3$.

$$923 = 13 \times 71,$$

where 71 is a prime of the form $4k+3$, and

$$17\,555 = 5 \times 3511,$$

where 3511 is a prime of the form $4k+3$. If we can prove that this is generally the case then we are home. We shall be able to construct from any n primes in the arithmetic progression, a larger prime which is also in the progression, and Euclid's argument by contradiction will be available to us.

But first we shall digress to present separately a subsidiary result needed in the proof.

Theorem 3.2

Any integer of the form $4k+3$ is divisible by a prime of this same form.

Proof of Theorem 3.2

The Division Algorithm tells us that any integer is of one of the four forms $4q$, $4q+1$, $4q+2$ or $4q+3$. Of these, $4q$ and $4q+2$ are even and so, with the exception of the prime 2, any number of either of these forms is composite. As $4k+3$ is not divisible by 2, it follows that it is either prime or is a product of two or more primes each of which is of one of the forms $4q+1$ or $4q+3$.

The identity

$$(4m+1)(4n+1) = 4(4mn+m+n)+1$$

shows that the product of any two numbers of the form $4q+1$ is itself of the form $4q+1$. It follows that any product of numbers of the form $4q+1$ is still of the form $4q+1$. Hence, if $4k+3$ were divisible only by primes of the form $4q+1$ it would, itself, be of the form $4q+1$, which is not the case. Therefore $4k+3$ must have a prime divisor of the form $4q+3$. ■

Although Theorem 3.2 concerned numbers of the form $4k+3$ the strategy of the proof can be applied to numbers in some other arithmetic progressions.

Problem 3.2

Show that any prime $p > 3$ must be of one of the forms $6q+1$ or $6q+5$, and hence prove that any number of the form $6k+5$ must have a prime divisor of this same form.

We now complete the proof to which we have been heading.

Theorem 3.3 Primes of the form 4k+3

There are infinitely many primes of the form $4k+3$, where k is an integer.

Proof of Theorem 3.3

Suppose, to the contrary, that there are only finitely many primes of the form $4k+3$, say $p_1, p_2, p_3, \ldots, p_n$. Consider the integer

$$N = 4(p_1 p_2 p_3 \ldots p_n) - 1 = 4(p_1 p_2 p_3 \ldots p_n - 1) + 3.$$

We observe that N is of the form $4k+3$, and so, by Theorem 3.2, there is a prime p of form $4k+3$ which divides N. As $p_1, p_2, p_3, \ldots, p_n$ are presumed to be the only primes of the form $4k+3$, the prime p must be one of this list, say $p = p_i$. But then p divides N and p divides $4(p_1 p_2 p_3 \ldots p_n)$ and so p divides the integer combination $4(p_1 p_2 p_3 \ldots p_n) - N = 1$. That is, p divides 1, which is a contradiction.

Hence there are infinitely many primes of the form $4k+3$. ■

With the exception of the number 2, all primes are odd. In turn the odd primes fall into two categories, namely those of the form $4k+1$ and those of the form $4k+3$. Below we have begun a characterization of the odd integers from 3 onwards.

prime $4k+1$		5				13		17						29				37		41					
composite				9			15			21		25	27			33	35		39			45		49	…
prime $4k+3$	3		7		11				19		23				31						43		47		…

Theorem 3.3 shows that there are infinitely many members in the bottom row. In addition there are certainly infinitely many composites, since any odd multiple of 3, except 3 itself, is an odd composite number. It seems inevitable, therefore, that we should enquire about the top row. Are there infinitely many primes of the form $4k+1$?

Pursuing the infinitely many primes of the form $4k+3$, these split into two categories namely those of the form $8k+3$ and those of the form $8k+7$.

prime $8k+3$	3		11	19			43		59	67			…
prime $8k+7$		7			23	31		47			71	79	…

At least one of these lists must be infinite. Are there infinitely many primes of the form $8k+3$? Are there infinitely many primes of the form $8k+7$?

All three questions posed above have affirmative answers. However, their proofs are not as elementary as the proof that there are infinitely many primes of the form $4k+3$ and we shall postpone these proofs until we have more mathematical tools at our disposal. Nevertheless there are other arithmetic progressions for which the question of the infinitude of primes can be easily resolved.

Problem 3.3

Making use of the result of Problem 3.2, modify the proof of Theorem 3.3 to prove that there are infinitely many primes of the form $6k+5$.

All these observations suggest a general question concerning primes in arithmetic progressions. Given *any* two positive integers a and b are there infinitely many primes of the form $ak+b$, where k is a non-negative integer?

Clearly the answer to this is no. Any common divisor of a and b divides each of the integer combinations $ak + b$, so to have a chance of generating primes we must add the stipulation that $\gcd(a, b) = 1$. Many of the great names of mathematics are associated with assaults on this problem, including Euler (who we shall meet in *Unit 5*). Euler conjectured, but could not prove, that there are infinitely many primes of the form $ak + 1$ for each positive integer a. The ultimate credit for solving this problem goes to Dirichlet, a student of Gauss (whom we shall meet in *Unit 3*), who in 1837 used methods of mathematical analysis to prove the result which bears his name.

Theorem 3.4 Dirichlet's Theorem

If a and b are positive integers with $\gcd(a, b) = 1$, then there are infinitely many primes of the form $ak + b$, where k is a non-negative integer.

The proof of Dirichlet's Theorem is well beyond the scope of this course.

Before leaving arithmetic progressions, we make the observation that the number of consecutive primes in any such progression is limited. To justify this remark consider the progression

$$a,\ a+b,\ a+2b,\ a+3b,\ \ldots,$$

and suppose that some term $a + rb$ is a prime, say p. Then every pth term thereafter is a multiple of p.

$$\begin{aligned}
&a + rb = p\\
&a + (r+p)b = p + pb = p(1+b)\\
&a + (r+2p)b = p + 2pb = p(1+2b)\\
&a + (r+3p)b = p + 3pb = p(1+3b)\\
&\vdots\\
&a + (r+np)b = p + npb = p(1+nb)
\end{aligned}$$

To illustrate what this argument says, consider the arithmetic progression of numbers of the form $4k + 1$, for $k \in \mathbb{Z}^+$. The first number is 5, which is prime. The argument tells us that every fifth term, that is, the 1st, 6th, 11th, 16th and so on, is divisible by 5, and so is composite. It follows that this sequence cannot have more than five consecutive members all of which are prime.

The numbers

$$7,\ 37,\ 67,\ 97,\ 127 \text{ and } 157$$

$a = 7$, $b = 30$

form a sequence of six primes in arithmetic progression, while the numbers

$$7,\ 157,\ 307,\ 457,\ 607,\ 757 \text{ and } 907$$

$a = 7$, $b = 150$

form a sequence of seven primes in arithmetic progression. It is not possible to obtain a sequence of more than seven primes in which the first term is 7, since the eighth term would be divisible by 7.

Diversion

Palindromic primes in arithmetic progression.

13931, 14741, 15551, 16361
70607, 73637, 76667, 79697
94049, 94349, 94649, 94949
1120211, 1123211, 1126211, 1129211
1820281, 1823281, 1826281, 1829281

3.3 Primes generated by polynomials

In looking at arithmetic progressions we are really looking at linear functions $f(n) = an + b$, where a and b are positive integers and the domain of f is the non-negative integers. We have seen that some such functions take infinitely many composite values, while others take infinitely many prime values. One question we might pose is whether we can find a simple function which takes only prime values, thereby generating some, or perhaps all, prime numbers. Since we know that such a function cannot be a linear function the next obvious candidates to try are the quadratic functions.

Whenever n is a multiple of b, $an + b$ is divisible by b and so, if $b \geq 2$, $an + b$ takes infinitely many composite values.

The table drawn up below lists values of the quadratic $n^2 + n + r$ for some odd integer values of r.

Table 3.1 Values of $n^2 + n + r$, for $r = 1,\ 7,\ 11$ and 17 and for $n = 0$ to 12

n	n^2+n+1	n^2+n+7	n^2+n+11	n^2+n+17
0	1	7	11	17
1	3	$9 = 3^2$	13	19
2	7	13	17	23
3	13	19	23	29
4	$21 = 3 \times 7$	$27 = 3^3$	31	37
5	31	37	41	47
6	43	$49 = 7^2$	53	59
7	$57 = 3 \times 19$	$63 = 3^2 \times 7$	67	73
8	73	79	83	89
9	$91 = 7 \times 13$	97	101	107
10	$111 = 3 \times 37$	$117 = 3^2 \times 13$	$121 = 11^2$	127
11	$133 = 7 \times 19$	139	$143 = 11 \times 13$	149
12	157	163	167	173

Primes appear to crop up quite frequently. In particular, all the listed values for $n^2 + n + 17$ are prime, as would be the values for $n = 13$, 14 and 15, had we listed them. However at $n = 16$ this quadratic at last takes a composite value, as $16^2 + 16 + 17 = 289 = 17^2$.

Even more interesting is the quadratic $f(n) = n^2 + n + 41$ whose first 40 values all turn out to be prime:

Table 3.2 $n^2 + n + 41$ is prime for $n = 0, 1, 2, \ldots, 39$

n	$f(n)$	n	$f(n)$	n	$f(n)$	n	$f(n)$
0	41	10	151	20	461	30	971
1	43	11	173	21	503	31	1033
2	47	12	197	22	547	32	1097
3	53	13	223	23	593	33	1163
4	61	14	251	24	641	34	1231
5	71	15	281	25	691	35	1301
6	83	16	313	26	743	36	1373
7	97	17	347	27	797	37	1447
8	113	18	383	28	853	38	1523
9	131	19	421	29	911	39	1601

In the Middle Ages it was widely believed that all the values taken by this quadratic were prime. However the next two numbers corresponding to $n = 40$ and $n = 41$ provide counter-examples.

$$f(40) = 40^2 + 40 + 41 = 41^2$$
$$f(41) = 41^2 + 41 + 41 = 41 \times 43$$

There is another, somewhat curious way in which the numbers arising from this quadratic can be viewed. Suppose that starting at 41 we write down the positive integers in an anticlockwise spiral, as indicated.

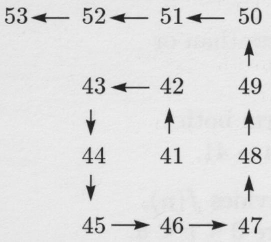

53 52 51 50
43 42 49
44 41 48
45 46 47

Figure 3.1 Spiralling around 41

Now we remove all the composites, leaving just primes behind, as shown in Figure 3.2.

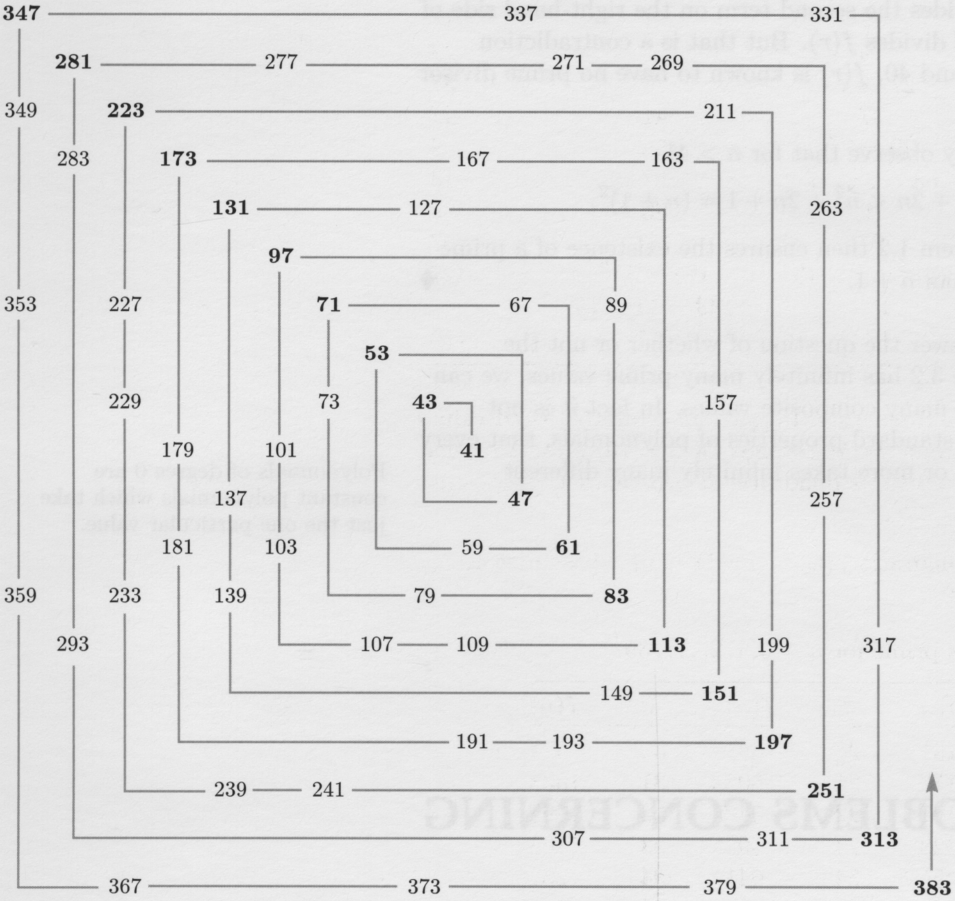

347 337 331
281 277 271 269
349 223 211
283 173 167 163
131 127 263
97
353 227 71 67 89
53
229 73 43 157
179 101 41
137 47 257
181 103 59 61
359 233 139 79 83
293 107 109 113 199 317
149 151
191 193 197
239 241 251
307 311 313
367 373 379 383

Figure 3.2 The primes from 41 to 383 in spiral formation

It appears that none of the terms on the diagonal from top left to bottom right are removed, and so are prime. They are in fact the values of $f(n)$. We leave you to convince yourself of the last statement and to wonder about the previous one.

It turns out that in the values of $n^2 + n + 41$ for $n = 0, 1, 2, \ldots, 100$ there are just 14 composite values and 87 primes. Nevertheless, to this day, it is not known whether this quadratic takes infinitely many prime values. (Indeed the same question has not yet been answered for the simpler quadratic $n^2 + 1$. Are there infinitely many primes which are 1 more than a square?) But we can say some things about divisors of $n^2 + n + 41$ as the next example shows.

Example 3.2

Show that:

(a) $f(n) = n^2 + n + 41$ does not have a prime divisor less than 41, for any value of n;

(b) if $f(n)$ is composite, then it has a prime divisor which is less than or equal to $n + 1$.

Table 3.2 together with $f(40) = 41^2$ and $f(41) = 41 \times 43$ confirm both claims for integers up to 41 so we need only consider integers $n > 41$.

Aiming for a contradiction to the first claim, suppose that d divides $f(n)$, where $1 < d < 41$. By the Division Algorithm $n = qd + r$, where $0 \leq r < d$. Therefore

$$\begin{aligned} f(n) &= (qd + r)^2 + (qd + r) + 41 \\ &= r^2 + r + 41 + q^2d^2 + 2dqr + qd \\ &= f(r) + d\left(q^2d + 2qr + q\right). \end{aligned}$$

Since d divides $f(n)$ and d divides the second term on the right-hand side of this equation, it follows that d divides $f(r)$. But that is a contradiction since, with r lying between 0 and 40, $f(r)$ is known to have no prime divisor less than 41.

For the second claim we simply observe that for $n > 41$

$$f(n) = n^2 + n + 41 < n^2 + 2n < n^2 + 2n + 1 = (n + 1)^2,$$

so, if $f(n)$ is composite, Theorem 1.2 then ensures the existence of a prime divisor of $f(n)$ which is less than $n + 1$.

◆

Although we are unable to answer the question of whether or not the quadratic function of Example 3.2 has infinitely many prime values, we can confirm that it takes infinitely many composite values. In fact it is not difficult to show, appealing to standard properties of polynomials, that every integer polynomial of degree 1 or more takes infinitely many different composite values.

Polynomials of degree 0 are constant polynomials which take just the one particular value.

4 FAMOUS PROBLEMS CONCERNING PRIMES

4.1 Proximity of primes

Ignoring the first two primes, 2 and 3, the closest together that two primes can be is 2, occurring when two consecutive odd numbers are both prime. Such pairs of primes are called *twin primes*:

$$3, 5;\ \ 5, 7;\ \ 11, 13;\ \ 17, 19;\ \ 29, 31;\ \ 41, 43;\ \ \ldots.$$

It is an unanswered question as to whether or not there are infinitely many pairs of twin primes although numerical evidence, gathered by computer, suggests there are.

Table 4.1 Twin primes

n	nth pair of twin primes
1000	79 559, 79 561
2000	182 027, 182 029
3000	300 497, 300 499
4000	424 769, 424 771
5000	557 519, 557 521
6000	690 887, 690 889
7000	833 099, 833 101
8000	974 537, 974 539
9000	1 115 417, 1 115 419
10 000	1 260 989, 1 260 991

Despite the frequency with which successive primes are as close together as possible, it is nevertheless the case that the gap between successive primes can be arbitrarily large, by which we mean that for any given positive integer n, no matter how large, there exist n consecutive integers all of which are composite. This is easily demonstrated. Consider the n consecutive integers

$$(n+1)!+2,\ (n+1)!+3,\ (n+1)!+4,\ \ldots,\ (n+1)!+(n+1),$$

where, as usual, $(n+1)! = (n+1) \times n \times \cdots \times 3 \times 2 \times 1$. The first of the listed numbers is divisible by 2, the second by 3, the third by 4, and so on, the last being divisible by $n+1$. So these n consecutive integers are all composite.

The same argument shows that the n consecutive numbers

$$(n+1)!-(n+1),\ (n+1)!-n,\ \ldots,\ (n+1)!-3,\ (n+1)!-2$$

are composite. So, for each positive integer n, of the $2n+3$ numbers consisting of $(n+1)!$ and the symmetrically surrounding numbers, namely

$$\begin{gathered}(n+1)!-(n+1),\ (n+1)!-n,\\ \ldots,(n+1)!-2,\ (n+1)!-1,\ (n+1)!,\ (n+1)!+1,\ (n+1)!+2,\\ \ldots,(n+1)!+n,\ (n+1)!+(n+1),\end{gathered}$$

all are composite with the possible exceptions of $(n+1)!-1$ and $(n+1)!+1$.

For instance, taking $n=4$, so that $(n+1)! = 120$, of the eleven numbers

$$115,\ 116,\ 117,\ 118,\ 119,\ 120,\ 121,\ 122,\ 123,\ 124,\ 125,$$

only the two either side of 120 can be prime. As it happens $119 = 7 \times 17$ and $121 = 11^2$, so all 11 are composite. Indeed we can tack 114 on the beginning and 126 on the end to obtain a sequence of 13 consecutive composite numbers. This shows that there are long sequences of composite numbers either side of $n!$. If, as for the case $n=5$, both of the numbers $n!+1$ and $n!-1$ are composite there will be even longer sequences of composites.

Problem 4.1

What is the longest sequence of consecutive composite numbers including $6! = 720$?

A table of primes is given in the Appendix to this unit.

The above considerations suggest that we might look with interest at the sequence of numbers $\{n!+1\}$, $n = 1, 2, 3, \ldots$. Is $n!+1$ prime for infinitely many n? This is yet another unsolved problem, although in *Unit 4* we shall prove a famous result which shows that $n!+1$ is composite infinitely often.

Moving on from pairs of primes, the next question to ask concerns whether it is possible for three consecutive odd integers to all be prime. Certainly $\{3, 5, 7\}$ is one such set of primes. But this is the only example, because, of three consecutive odd integers one of them must be divisible by 3. We ask you to establish this in the next problem.

Problem 4.2

Suppose that n, $n+2$ and $n+4$ are three consecutive odd integers. Use the fact that n must be of one of the forms $3k$, $3k+1$ or $3k+2$ to show that one of n, $n+2$ or $n+4$ is divisible by 3.

The best that we can do with three primes is to find instances of four consecutive odd numbers three of which are prime, such as

$$5, 7, 11;\ 7, 11, 13;\ 11, 13, 17;\ 13, 17, 19;\ 17, 19, 23;\ 37, 41, 43;\ \ldots.$$

Such trios of primes are called *prime triplets.* Note that each prime triplet contains a pair of twin primes.

Moving on one stage, we can have two pairs of twin primes with just one missing odd number between them, so that of five consecutive odd numbers four are prime:

$$5, 7, 11, 13;\ 11, 13, 17, 19;\ 101, 103, 107, 109;\ 191, 193, 197, 199;\ \ldots.$$

These are examples of *prime quartets.* Prime quartets are, of course, relatively rare in comparison with twin primes and yet numerical evidence leads to a belief that, still, there are infinitely many prime quartets.

Amongst the integers up to one million there are 166 sets of prime quartets.

4.2 The Goldbach Conjecture

We now consider a problem which is arguably the most famous unsolved problem concerning primes: the so-called Goldbach Conjecture. Its fascination stems from the fact that numerical evidence suggests that it is manifestly true, and yet no one has managed to prove it to this day.

Goldbach Conjecture

Every even integer from 6 onwards can be written as a sum of two odd primes.

The first ten even integers from 6 onwards, are expressed as a sum of two odd primes as follows.

$6 = 3 + 3$

$8 = 3 + 5$

$10 = 3 + 7 = 5 + 5$

$12 = 5 + 7$

$14 = 3 + 11 = 7 + 7$

$16 = 3 + 13 = 5 + 11$

$18 = 5 + 13 = 7 + 11$

$20 = 3 + 17 = 7 + 13$

$22 = 3 + 19 = 5 + 17 = 11 + 11$

$24 = 5 + 19 = 7 + 17 = 11 + 13$

Notice that some of the even integers have several different expressions as the sum of two primes.

Problem 4.3

Express each of the even numbers from 40 to 60 inclusive as a sum of two odd primes.

Computers have verified Goldbach's Conjecture for even integers up to 10^8 (in 1965), but little headway has been made towards a general proof. The most significant development in this direction was due to a Russian mathematician Vinogradov who, in 1937, proved that every sufficiently large odd integer is the sum of three primes (so that every large enough even integer is a sum of at most four primes). However, by sufficiently large we are talking of numbers in excess of $3^{3^{15}} \simeq 10^{6\,846\,169}$, which leaves rather a lot of numbers smaller than this still to be checked, and the size of these numbers is still well beyond the capabilities of even the most modern computers.

4.3 The Prime Number Theorem

We have seen plenty of evidence for the unpredictability of occurrences of prime numbers. On the one hand there appear to be infinitely many pairs of consecutive odd integers both of which are prime, whilst at the same time there are arbitrarily long sequences of consecutive integers all of which are composite. But, despite this local irregularity of their distribution, when we look at the primes overall, their global distribution can be described with rather more success.

Towards the end of the eighteenth century Gauss observed that near an integer x, the probability that a number is prime is approximately $\dfrac{1}{\log x}$; to be more precise, in the interval from x to $x+N$, (where N is neither too large nor too small), the number of primes is about $\dfrac{N}{\log x}$. For example, if $x = 10^7$ and $N = 5000$, then

$$\frac{5000}{\log(10^7)} = \frac{5000}{7\log 10} \simeq 310.2,$$

and there are actually 305 primes between 10 000 000 and 10 005 000.

In this course log will always mean the natural logarithm, $\log_e$, sometimes denoted by ln.

This led Gauss, still only 15 years of age, to conjecture a result which has become one of the most notorious results of mathematics. When looking at the density of primes in intervals an important function for consideration is $\pi(x)$, defined for each positive real number x to be the number of primes not exceeding x. So, for example, $\pi(6) = 3$ and $\pi(10\sqrt{2}) = 6$. Gauss observed similarities between $\pi(x)$ and the logarithmic integral

$$\mathrm{Li}(x) = \int_2^x \frac{1}{\log t}\,dt.$$

Gauss had tables of primes up to three million and he compiled a list of the number of primes occurring in consecutive groups of 1000. The table below provides much more evidence. In it, $\mathrm{Li}(x)$ has been rounded to the nearest integer.

Table 4.2 Density of primes

x	$\pi(x)$	$\mathrm{Li}(x)$
100	25	30
1000	168	178
10 000	1229	1246
100 000	9592	9630
1 000 000	78 498	78 628
10^7	664 579	664 918
10^8	5 761 455	5 762 209
10^{10}	455 052 511	455 055 615
10^{12}	37 607 912 018	37 607 950 281
10^{14}	3 204 941 750 802	3 204 942 065 692

Our values for $\mathrm{Li}(x)$ were determined using the mathematical software package Maple.

The result that Gauss noticed was eventually proved in 1896, almost 100 years after he first conjectured it:

The Prime Number Theorem

$$\lim_{x\to\infty} \frac{\pi(x)}{\mathrm{Li}(x)} = 1$$

The determination of $\pi(x)$ involves finding all the primes less than or equal to x. In contrast, $\mathrm{Li}(x)$ can be calculated even for large x by any of the standard ways of approximating integrals. The Prime Number Theorem confirms what is indicated in the above table, namely, that for large x, $\mathrm{Li}(x)$ is a very good approximation to $\pi(x)$.

Gauss was unable to prove the Prime Number Theorem. It was through the collective genius and hard work of several mathematicians in the nineteenth century, notably Dirichlet, Tchebychef, Riemann, Hadamard and de la Vallée Poussin, that the theorem was finally proved in 1896 by Hadamard, and, independently, by de la Vallée Poussin.

The proofs of the Prime Number Theorem given at that time made extensive use of complex function theory, utilizing properties of the so-called Riemann zeta function. But in 1949, a purely algebraic proof, not calling on techniques of complex analysis, was discovered by the Norwegian mathematician Selberg. This proof, however, is extremely complicated and beyond the scope of this, or any other, first course in Number Theory.

On route to proving the Prime Number Theorem by methods of complex analysis, many other results emerge which are interesting in their own right. Two results merit mention here. Many students of mathematics are surprised on first learning that the harmonic series

$$\sum_{n\geq 1} \frac{1}{n} = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} + \cdots$$

is divergent (the sum is unbounded). So, it must come as a real shock to learn that if all the terms are discarded except those where the denominator is prime, then the resulting series

$$\sum_{p\text{ prime}} \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \cdots + \frac{1}{p} + \cdots$$

is *still* divergent. And yet, despite the firm belief that there are infinitely many pairs of twin primes, if we discard all the terms of the harmonic series except those where the denominator belongs to a pair of twin primes, then the resulting series

$$\sum_{\substack{p\text{ twin}\\ \text{prime}}} \frac{1}{p} = \frac{1}{3} + \frac{1}{5} + \frac{1}{7} \cdots + \frac{1}{29} + \frac{1}{31} + \cdots$$

converges with sum less than 2.

5 FIBONACCI NUMBERS

5.1 The Fibonacci sequence

We have investigated occurrences of primes in sequences

$$f(1), f(2), f(3), \ldots,$$

where f is a polynomial with integer coefficients. A further step along this road is to investigate occurrences of primes in recursive sequences, that is, sequences defined by recurrence relations. We shall restrict ourselves to considering just the best known of all such sequences, the Fibonacci sequence. This sequence has many interesting properties, which we shall investigate along with its connections with primes.

In his book *Liber Abaci*, written in 1202, Fibonacci posed the following problem.

> A pair of rabbits, one male and one female, are confined to an area. The nature of the rabbits is that they produce, on the last day of each month from the second month onwards, a pair of rabbits which, in turn, reproduce in the same way. Assuming that no rabbits die, how many pairs will there be on the first day of each month.

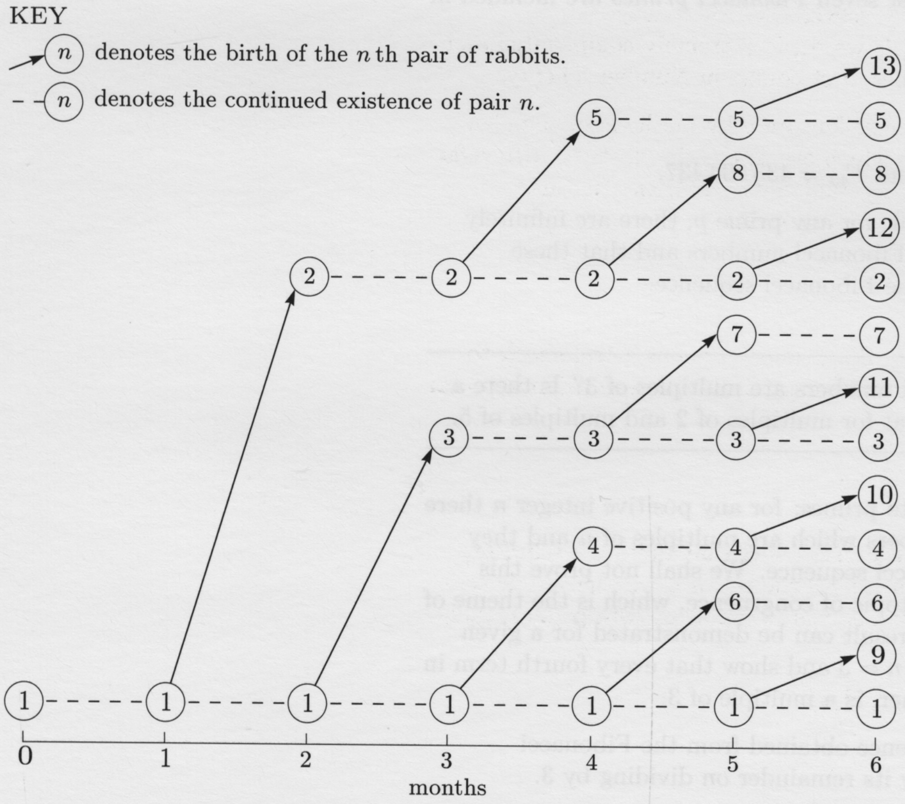

KEY
n denotes the birth of the n th pair of rabbits.
n denotes the continued existence of pair n.
1
2
3
4
5
6
7
8
9
10
11
12
13
0
1
2
3
4
5
6
months

Figure 5.1 Breeding rabbit pairs

Figure 5.1 shows how the rabbits will breed for the first six months. The dotted lines indicate the continued existence of a pair of rabbits while the arrowed lines indicate the birth of another pair at the end of that month.

If we denote the number of pairs of rabbits alive during month n by F_n, then F_{n+2} is obtained by adding to F_{n+1} the number of births at the end of month $n+1$. Now there is one birth at the end of month $n+1$ for each of the F_n pairs alive during month n. Hence the sequence of numbers $\{F_n\}$ is defined by

$$F_1 = F_2 = 1; \text{ and } F_{n+2} = F_{n+1} + F_n, \quad \text{for } n \geq 1.$$

That is, each term, from the third onwards, is the sum of the previous two terms.

We shall refer to the numbers arising in this sequence as *Fibonacci numbers.* The first twenty Fibonacci numbers are given in the following table.

Table 5.1 The Fibonacci numbers F_1 to F_{20}

$F_1 = 1$	$F_6 = 8$	$F_{11} = 89$	$F_{16} = 987$
$F_2 = 1$	$F_7 = 13$	$F_{12} = 144$	$F_{17} = 1597$
$F_3 = 2$	$F_8 = 21$	$F_{13} = 233$	$F_{18} = 2584$
$F_4 = 3$	$F_9 = 34$	$F_{14} = 377$	$F_{19} = 4181$
$F_5 = 5$	$F_{10} = 55$	$F_{15} = 610$	$F_{20} = 6765$

On noticing that each of $F_3 = 2$, $F_5 = 5$, $F_7 = 13$ and $F_{11} = 89$ is prime, one is lured towards the conjecture that F_p will be prime whenever p is an odd prime. However this possibility is shot down just a little further along the sequence:

$$F_{19} = 4181 = 37 \times 113.$$

The occurrences of primes in the Fibonacci sequence pose numerous problems, many of which remain unsolved. In particular, it is believed, but not yet proved, that there are infinitely many prime Fibonacci numbers despite their relative rarity. The first seven *Fibonacci primes* are included in the above list,

2, 3, 5, 13, 89, 233 and 1597.

The next three are

$$F_{23} = 28\,657, \ F_{29} = 514\,229 \text{ and } F_{43} = 433\,494\,437.$$

On the positive side it is known that, for any prime p, there are infinitely many multiples of p which arise as Fibonacci numbers and that these multiples occur equally spaced in the Fibonacci sequence.

Problem 5.1

Which of the first twenty Fibonacci numbers are multiples of 3? Is there a pattern to where they occur? Repeat for multiples of 2 and multiples of 5.

The result just cited is not special to primes: for any positive integer n there are infinitely many Fibonacci numbers which are multiples of n and they occur equally spaced in the Fibonacci sequence. We shall not prove this result here but, as a lead in to the topic of congruence, which is the theme of *Unit 3*, we shall illustrate how the result can be demonstrated for a given value of n. We begin with the case $n = 3$ and show that every fourth term in the Fibonacci sequence, and no other, is a multiple of 3.

We start by writing down the sequence obtained from the Fibonacci sequence by replacing each term by its remainder on dividing by 3.

$$1,\ 1,\ 2,\ 0,\ 2,\ 2,\ 1,\ 0,\ 1,\ 1,\ 2,\ 0,\ 2,\ 2,\ 1,\ 0,\ \ldots.$$

By the Division Algorithm the terms can only be 0, 1 or 2, where the zeros correspond to the Fibonacci numbers which are divisible by 3. As you can see, so far every fourth term (and no other) is a zero, and what we need to prove is that this pattern continues. The essence of the argument is that we can continue the new (remainder) sequence without reference to the original Fibonacci numbers. As each Fibonacci number is the sum of the previous two, it follows that each term of the remainder sequence is obtained by adding the two previous remainders (and subtracting 3 if necessary). For example, successive terms 2 and 1 in the remainder sequence correspond to

Fibonacci numbers of the respective forms $3k + 2$ and $3l + 1$ and the next term,

$$(3k + 2) + (3l + 1) = 3(k + l + 1) + 0,$$

has remainder 0 on division by 3. Our observation merely states that this remainder could have been obtained directly by adding the remainders 2 and 1, and taking the remainder of this resulting sum on dividing by 3. (We shall ask you to prove a general result of this type in Problem 5.2.)

The proof is completed by noting that the remainder sequence consists of the pattern 1, 1, 2, 0, 2, 2, 1, 0 recurring indefinitely, since once a pair of consecutive numbers is a repetition of an earlier pair (as will be the pair 1, 1 in this example) the pattern must recur. Hence the zeros in the remainder sequence occur every fourth term and the corresponding Fibonacci numbers are the ones divisible by 3.

This same of line of attack can be used to find where the multiples of any integer n occur in the Fibonacci sequence.

Problem 5.2

Suppose that the integers a and b have remainders r and s on dividing by the positive integer n. Show that $a + b$ and $r + s$ have the same remainder on dividing by n.

Problem 5.3

Write out the sequence of remainders obtained when the terms of the Fibonacci sequence are divided by (i) 6, and (ii) 7, and hence find where the multiples of 6 and 7 occur in the Fibonacci sequence.

5.2 Properties of Fibonacci numbers

If it happened that two consecutive Fibonacci numbers were divisible by a common prime p then the sequence of remainders constructed for that prime p would contain consecutive zeros, and hence all terms thereafter would be 0. It is clear that this does not happen since to obtain two consecutive zeros, the previous term would have had to be 0 and, working our way back, the first term would have had to be 0, which it is not. Therefore consecutive Fibonacci numbers are relatively prime.

If $p \mid F_n$ and $p \mid F_{n+1}$, then $p \mid (F_{n+1} - F_n)$. That is, $p \mid F_{n-1}$.

There is a nice demonstration of this fact using the Euclidean Algorithm. If we apply the Euclidean Algorithm to find $\gcd(F_{n+1}, F_n)$, the equations involved, except the last, are no more than expressions that each Fibonacci number is the sum of the previous two.

$$\begin{array}{lll}
F_{n+1} = 1 \times F_n & + F_{n-1} & 0 < F_{n-1} < F_n \\
F_n = 1 \times F_{n-1} & + F_{n-2} & 0 < F_{n-2} < F_{n-1} \\
F_{n-1} = 1 \times F_{n-2} & + F_{n-3} & 0 < F_{n-3} < F_{n-2} \\
\quad\vdots & & \\
F_4 = 1 \times F_3 & + F_2 & 0 < F_2 < F_3 \\
F_3 = 2 \times F_2 & + 0 &
\end{array}$$

$F_3 = 2,\ F_2 = 1.$

The last non-zero remainder is $F_2 = 1$ and so we have proved the following result.

Theorem 5.1 The relative primeness of consecutive Fibonacci numbers

For any positive integer n,

$$\gcd(F_{n+1}, F_n) = 1.$$

There are many curious identities involving the Fibonacci numbers, a small sample of which we shall introduce here. Our ambitions in this section are directed towards divisibility properties of Fibonacci numbers. One identity which will prove to be very useful is:

A useful relationship between Fibonacci numbers

For all integers $m \geq 2$ and $n \geq 1$,

$$F_{m+n} = F_{m-1}F_n + F_mF_{n+1}.$$

For instance, putting $m = 7$ and $n = 5$, this identity gives,

$$F_{12} = F_{7+5} = F_6F_5 + F_7F_6 = 8 \times 5 + 13 \times 8 = 144,$$

and putting $m = 9$ and $n = 3$,

$$F_{12} = F_{9+3} = F_8F_3 + F_9F_4 = 21 \times 2 + 34 \times 3 = 144.$$

The general identity can be proved using the Second Principle of Mathematical Induction, as we now show.

Example 5.1

Prove that for all integers $m \geq 2$ and $n \geq 1$,

$$F_{m+n} = F_{m-1}F_n + F_mF_{n+1}.$$

We prove the result by induction on n. To this end, let $m \geq 2$ be a fixed integer and let $P(n)$ be the proposition that

$$F_{m+n} = F_{m-1}F_n + F_mF_{n+1}.$$

The proposition $P(1)$ states that

$$F_{m+1} = F_{m-1}F_1 + F_mF_2.$$

However, since $F_1 = F_2 = 1$, this is true, being exactly the way that the Fibonacci number F_{m+1} is defined as the sum of its two predecessors. Hence we have verified the basis for the induction.

We now assume that the the proposition $P(n)$ is true for $n = 1, 2, \ldots, k$ and proceed to establish its truth when $n = k + 1$. The inductive assumptions, for the cases $n = k - 1$ and $n = k$, are that

$$F_{m+k} = F_{m-1}F_k + F_mF_{k+1}$$

and that

$$F_{m+(k-1)} = F_{m-1}F_{k-1} + F_mF_k.$$

Adding these two we obtain

$$F_{m+k} + F_{m+(k-1)} = F_{m-1}(F_k + F_{k-1}) + F_m(F_{k+1} + F_k).$$

The sum on the left side of this equation and the two bracketed sums on the right are each the sum of consecutive Fibonacci numbers, and so, by definition,

$$F_{m+(k+1)} = F_{m-1}F_{k+1} + F_mF_{(k+1)+1}.$$

This shows that the proposition $P(k + 1)$ is true as it is the required formula with $n = k + 1$.

Hence, by Mathematical Induction,

$$F_{m+n} = F_{m-1}F_n + F_mF_{n+1} \quad \text{for all } m \geq 2 \text{ and } n \geq 1.$$

◆

This argument applies for any $m \geq 2$.

The formula established in Example 5.1 helps us to prove the following:

Theorem 5.2 Divisibility property of the Fibonacci numbers

For all integers $n > 2$, F_m is divisible by F_n if, and only if, m is divisible by n.

We first remark that the case $n = 2$ has to be excluded because $F_2 = 1$, and so every Fibonacci number is divisible by F_2, whilst it certainly is not the case that every integer m is divisible by 2.

Proof of Theorem 5.2

First we show that, if m is a multiple of n, then F_m is a multiple of F_n. To be precise, we shall show that F_{nq} is a multiple of F_n, for all integers $q \geq 1$, and this we do using Mathematical Induction.

The result is trivially true when $q = 1$ as it claims that F_n divides F_n. So we have a basis for the induction.

For the induction step, suppose that F_{nq} is divisible by F_n for $q = 1, 2, \ldots, k$. We require to prove that $F_{n(k+1)}$ is divisible by F_n. The useful relationship between Fibonacci numbers proved in Example 5.1 gives

$$F_{n(k+1)} = F_{nk+n} = F_{nk-1}F_n + F_{nk}F_{n+1}.$$

By the induction hypothesis F_n divides F_{nk} and so F_n divides each of the terms on the right-hand side of this equation. Hence F_n divides $F_{n(k+1)}$ which completes the induction step.

Hence, by the Second Principle of Mathematical Induction, F_{nq} is is a multiple of F_n for all integers $q \geq 1$.

Conversely, we suppose that F_m is divisible by F_n and then have to prove that m is divisible by n. Aiming for a contradiction, suppose $m = nq + r$, where $1 \leq r < n$. Then

It is an 'if, and only if,' claim so we require proof in the opposite direction too.

$$F_m = F_{nq+r} = F_{nq-1}F_r + F_{nq}F_{r+1}.$$

Now we have just seen, in the first part, that F_{nq} is divisible by F_n and so, as F_m is also divisible by F_n, it follows that F_n divides $F_{nq-1}F_r$. If we can show that $\gcd(F_{nq-1}, F_n) = 1$ the proof will be complete, because then Euclid's Lemma tells us that F_n divides F_r, an obvious contradiction because $F_n > F_r > 0$.

From its construction $\{F_n\}$ is an increasing sequence once $n \geq 2$.

To plug the remaining hole, let $\gcd(F_{nq-1}, F_n) = d$. Then d divides F_n, and so d divides F_{qn}. But then d divides F_{qn-1} and d divides F_{qn}, so d is a common divisor of consecutive Fibonacci numbers. Hence, by Theorem 5.1, $d = 1$ as required. ■

We claimed earlier that, for any integer $a \geq 1$, infinitely many multiples of a occur in the Fibonacci sequence with equal spacing. Theorem 5.2 has taken us some distance towards a proof of that result. Suppose that the first Fibonacci number which is a multiple of a is F_n. Then F_n, F_{2n}, F_{3n}, $\ldots$ are equally spaced multiples of a. But are they the only ones?

Problem 5.4

Suppose that F_n is the first Fibonacci number which is a multiple of a positive integer a. Show that if F_m is a multiple of a then m is a multiple of n. *Hint*: Write $m = nq + r$ and use the 'useful relationship' as in the proof of Theorem 5.2

What we have still not shown is that a multiple of a will definitely occur. That proof will have to be postponed until another occasion. We shall leave Fibonacci for now with two final problems for you.

Problem 5.5

It is known that for any prime $p > 5$ either F_{p-1} or F_{p+1} is divisible by p. Confirm that this is true for all primes up to 19.

Problem 5.6

Show that $F_n^2 = F_{n+1}F_n - F_nF_{n-1}$ for all integers $n \geq 2$.

Deduce that the sum of the squares of the first n Fibonacci numbers satisfies

$$F_1^2 + F_2^2 + F_3^2 + \cdots + F_n^2 = F_{n+1}F_n.$$

ADDITIONAL EXERCISES

Section 1

1 Find the prime decomposition of 20!

2 Given that p and q are distinct primes such that their product pq divides a^n, prove that $(pq)^n$ divides a^n.

3 Prove that the only prime p for which $3p + 1$ is a square is $p = 5$.

4 Show that for any prime p, $8p - 1$ and $8p + 1$ cannot both be prime.

5 Let $p \geq 5$ be prime. Show that the remainder on dividing p by 12 must be one of 1, 5, 7 or 11. Hence prove that if $p \geq q \geq 5$ are primes then $24|(p^2 - q^2)$.

6 Prove (as Cataldi did in 1588) that if a is a positive integer and $n \geq 2$ such that $a^n - 1$ is prime then $a = 2$ and n is prime. *Hint*: Consider the factorization $a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \cdots + a + 1)$.

Section 2

1 Let $m = 2^3 \times 3^2 \times 7 \times 11$ and $n = 3344$. Determine the prime decomposition of $\gcd(m, n)$ and $\operatorname{lcm}(m, n)$.

2 Write down, in terms of primes p, q, etc, the prime decompositions of all positive integers which have eight divisors including the integer itself and 1. Hence find all positive integers less than 100 which have eight divisors.

3 A positive integer n is said to be a *practical number* if every positive integer r in the range $1 \leq r \leq n$ can be written as a sum of one or more distinct positive divisors of n.

(a) Which of the following are practical?

6, 10, 12, 14, 16.

(b) Prove that for each integer $n \geq 1$, the number 2^n, is a practical number.

In future we may not be so particular about including the phrase 'one or more' and will automatically allow the possibility of a sum to contain only one number.

Section 3

1 Suppose that there are only finitely many primes, say $p_1, p_2, p_3, \ldots, p_n$. Show that the number $p_1 + p_2p_3 \ldots p_n$ is not divisible by any prime in the given list. What can you deduce from this observation?

2 Prove that if three prime numbers, all greater than 3, form an arithmetic progression then the common difference of the progression is a multiple of 6. What can you say about the common difference in an arithmetic progression of five primes?

3 Consider the sequence of integers $\{n^2 + 3\}$, $n \geq 1$:

4, 7, 12, 19, 28, 39, 52, 67, 84, ...

Prove that consecutive terms of this sequence are either relatively prime or have a greatest common divisor of 13.

Section 4

1 Show that the sum of twin primes p and $p+2$, where $p > 3$, is divisible by 12.

2 If n, $n+2$, $n+6$ and $n+8$ is a prime quartet, where $n > 5$, what is the remainder when n is divided by 15?

3 Prove that Goldbach's Conjecture is equivalent to the following statement.

> Every integer greater than or equal to 6 is a sum of three primes.

4 Prove that every even integer from 40 onwards can be expressed as the sum of two odd composite numbers. *Hint*: All the numbers of the form $10k$ can be written as $15 + (10k - 15)$.

Section 5

1 Use the 'useful relationship between Fibonacci numbers' to determine F_{22}, F_{23} and F_{24} from the values $F_{10} = 55$, $F_{11} = 89$ and $F_{12} = 144$. Confirm that F_{11} divides F_{22} and that each of F_4, F_6, F_8, and F_{12} divides F_{24}.

2 (a) Which Fibonacci numbers are multiples of 13?
(b) Show that 4 divides F_n if, and only if, 8 divides F_n.

3 Prove the following identities concerning sums of Fibonacci numbers.
(a) $F_1 + F_2 + F_3 + \cdots + F_n = F_{n+2} - 1$.
(b) $F_1 + F_3 + F_5 + \cdots + F_{2n-1} = F_{2n}$.
(c) $F_2 + F_4 + F_6 + \cdots + F_{2n} = F_{2n+1} - 1$.

4 (a) Prove that if 2 divides F_n then 4 divides $F_{n+1}^2 - F_{n-1}^2$.
(b) Prove that if 3 divides F_n then 9 divides $F_{n+1}^3 - F_{n-1}^3$.

5 Prove that every positive integer can be written as a sum of one or more *distinct* Fibonacci numbers. *Hint*: Use induction on the claim that, for $n \geq 3$, each integer up to $F_n - 1$ can be written as a sum of one or more distinct numbers from the set $\{F_1, F_2, F_3, \ldots, F_{n-1}\}$.

Challenge Problems

1 Find all positive integers n which have the property that n is divisible by every integer r in the range $1 \leq r \leq \sqrt{n}$.

2 Prove that $n^4 + 4^n$ is composite for every integer $n \geq 2$.

3 Evaluate each of the following.

(a) $\displaystyle\sum_{n\geq 1} \frac{1}{F_n F_{n+2}}$ (b) $\displaystyle\sum_{n\geq 1} \frac{F_n}{10^n}$

4 Prove that the greatest common divisor of two Fibonacci numbers is itself a Fibonacci number. To be specific, prove that $\gcd(F_m, F_n) = F_{\gcd(m,n)}$.

SOLUTIONS TO THE PROBLEMS

Solution 1.1

As $11^2 > 117$ we need only test each of the given numbers for divisibility by 2, 3, 5 and 7.
111 is divisible by 3, and so is composite.
113 is not divisible by 2, 3, 5 or 7 and so is prime.
115 is divisible by 5 and so is composite.
117 is divisible by 3 and so is composite.

Solution 1.2

$22 < \sqrt{499} < 23$ so it is sufficient to check divisibility by the primes not exceeding 22; that is by 2, 3, 5, 7, 11, 13, 17 and 19.

Solution 1.3

The primes which do not exceed $\sqrt{200}$ are 2, 3, 5, 7, 11 and 13 so we must cross out all the multiples of these primes occurring in the list of 60 numbers from 141 to 200. The first multiple of 2 in this list is 142, so we cross out 142 and every second number. The first multiple of 3 is 141 so we cross this out along with every third number following it. Similarly we cross out 145 and every fifth number, 147 and every seventh number, 143 and every eleventh number and 143 and every thirteenth number. The numbers that remain uncrossed out are the primes:

$$149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197 \text{ and } 199.$$

Solution 1.4

$$168 = 2^3 \times 3 \times 7$$
$$226 = 2 \times 113$$
$$36000 = 2^5 \times 3^2 \times 5^3$$

Solution 1.5

On the one hand if each exponent is even, say $k_i = 2l_i$, then

$$n = p_1^{2l_1} p_2^{2l_2} \ldots p_r^{2l_r} = \left(p_1^{l_1} p_2^{l_2} \ldots p_r^{l_r}\right)^2$$

is a square.

On the other hand if n is a square, say $n = a^2$, then writing $a = q_1^{m_1} q_2^{m_2} \ldots q_t^{m_t}$ in its prime decomposition and squaring gives

$$n = q_1^{2m_1} q_2^{2m_2} \ldots q_t^{2m_t}.$$

As the q_i are distinct primes and each m_i is positive, this is the unique prime decomposition of n, it reveals that each exponent is even.

Note that a simple modification of this argument generalizes the result to any power; an integer is an nth power if, and only if, each of its prime exponents is a multiple of n.

Solution 1.6

If $n^3 - 1$ is prime then the given identity expresses a prime as a product of two divisors. The uniqueness of prime decomposition tells us that this cannot happen unless one of these divisors is 1. Now $n > 1$ (since $n^3 - 1$ is prime) and so $n^2 + n + 1 \geq 3$. The only possibility is that $n - 1 = 1$, giving $n = 2$ and $n^3 - 1 = 7$.

Solution 2.1

There are in all 18 divisors of 252, including itself and 1, but what you should observe is that the prime decomposition of each divisor d involves only the primes 2, 3 and 7. What is more, since 2^3 does not divide 252 the exponent of 2 in the divisor d must be less than 3. Similarly the exponent of 3 in d cannot exceed 2 and the exponent of 7 in d cannot exceed 1. The conclusion to be drawn is that the divisors of 252 are the integers $2^r \times 3^s \times 7^t$, where $r = 0$, 1 or 2, $s = 0$, 1 or 2 and $t = 0$ or 1. The three choices for r, three choices for s and two choices for t give a total of $3 \times 3 \times 2 = 18$ divisors which are distinct due to the uniqueness of prime decomposition.

Solution 2.2

(a) The divisors of m are the integers $3^r \times 5^s \times 17^t$, where $0 \leq r \leq 3$, $0 \leq s \leq 1$ and $0 \leq t \leq 2$. That makes $4 \times 2 \times 3 = 24$ divisors in all.

The same reasoning gives $2 \times 3 \times 2 \times 5 = 60$ divisors of n.

(b) The common divisors of m and n are

$$1,\ 3,\ 3^2,\ 17,\ 3 \times 17,\ 3^2 \times 17,\ 17^2,\ 3 \times 17^2 \text{ and } 3^2 \times 17^2.$$

(c) The answer in part (b) lists all the common divisors of m and n, the largest one, $3^2 \times 17^2$, being the required value of $\gcd(m, n)$.

$$\begin{aligned}\operatorname{lcm}(m,n) &= \frac{mn}{\gcd(m,n)}\\ &= \frac{3^3 \times 5 \times 17^2 \times 2 \times 3^2 \times 7 \times 17^4}{3^2 \times 17^2}\\ &= 2 \times 3^3 \times 5 \times 7 \times 17^4.\end{aligned}$$

Solution 2.3

The six primes 2, 3, 5, 7, 11 and 19 are involved in m or n. For the greatest common divisor we write down the lower exponent (possibly 0) for each prime, while for the least common multiple we write down the larger exponent of each prime:

$$\gcd(m,n) = 2^0 \times 3^2 \times 5^0 \times 7^0 \times 11^1 \times 19^0 = 3^2 \times 11;$$
$$\operatorname{lcm}(m,n) = 2 \times 3^3 \times 5^3 \times 7 \times 11 \times 19.$$

Solution 2.4

24 can be expressed as a product of divisors in the following ways:

$$24,\ 2 \times 12,\ 2 \times 2 \times 6,\ 2 \times 3 \times 4,\ 2 \times 2 \times 2 \times 3,\ 3 \times 8,\ 4 \times 6.$$

Accordingly, a number with any of the following prime decompositions will have 24 divisors:

$$p_1^{23},\ p_1 p_2^{11},\ p_1 p_2 p_3^5,\ p_1 p_2^2 p_3^3,\ p_1 p_2 p_3 p_4^2,\ p_1^2 p_2^7,\ p_1^3 p_2^5.$$

The smallest of each type is, respectively:

$$2^{23},\ 2^{11} \times 3,\ 2^5 \times 3 \times 5,\ 2^3 \times 3^2 \times 5,\ 2^2 \times 3 \times 5 \times 7,\ 2^7 \times 3^2,\ 2^5 \times 3^3.$$

The smallest of these is $2^3 \times 3^2 \times 5 = 360$.

Solution 3.1

Let $P(n)$ be the proposition that the nth prime p_n is less than 2^n.

$P(2)$ is true since the second prime $p_2 = 3$ and $3 < 2^2$, giving the basis for the induction.

Suppose that, for some integer $k \geq 2$, $P(k)$ is true. That is,

$$p_k < 2^k.$$

By Bertrand's Conjecture, there is a prime, say q, lying between 2^k and 2^{k+1}. Putting the two facts together

$$p_k < 2^k < q < 2^{k+1}.$$

Now, as q is a prime exceeding p_k,

$$p_{k+1} \leq q,$$

and so

$$p_{k+1} < 2^{k+1},$$

which is $P(k+1)$, completing the proof.

Solution 3.2

Any integer takes of one of the six forms $6q$, $6q+1$, $6q+2$, $6q+3$, $6q+4$ or $6q+5$. Of these, $6q$, $6q+2$ and $6q+4$ are even while $6q+3$ is divisible by 3. Hence, with the exception of primes 2 and 3, any prime is of one of the forms $6q+1$ or $6q+5$.

The identity

$$(6m+1)(6n+1) = 6(6mn+m+n)+1$$

shows that the product of numbers of the form $6q+1$ is itself of this form. Therefore the number $6k+5$, which is not divisible by either 2 or 3, cannot have all its prime divisors of the form $6q+1$ and so must be divisible by a prime of form $6q+5$.

Solution 3.3

Suppose to the contrary that there are only finitely many primes of the form $6k+5$, say, $p_1, p_2, p_3, \ldots, p_n$, and consider the number

$$N = 6(p_1p_2p_3 \ldots p_n) - 1 = 6(p_1p_2p_3 \ldots p_n - 1) + 5.$$

We observe that N is of the form $6k+5$, and so by Problem 3.2 there is a prime p of form $6k+5$ which divides N. As $p_1, p_2, p_3, \ldots, p_n$ are presumed to be the only primes of the form $6k+5$, p must be one of this list, say $p = p_i$. But then p is a divisor of N and also of $6(p_1p_2p_3 \ldots p_n)$ and so p divides $6(p_1p_2p_3 \ldots p_n) - N$, that is, p divides 1, giving the required contradiction.

Solution 4.1

For the case $n = 5$, giving $(n+1)! = 720$, there are sequences of five consecutive composite numbers either side of 720. To be specific, we know that 714, 715, 716, 717, 718, 720, 722, 723, 724, 725 and 726 are composite. Of the two missing numbers 719 is prime — you might have tested divisibility by each of the primes from 2 to 23 inclusive, though reference to the table of primes given in the Appendix would have eased your task — and 721 is composite, being divisible by 7. The sequence of seven consecutive composites from 720 to 726 inclusive does not extend because the next higher number, 727, is also prime.

Solution 4.2

If $n = 3k$ then n is divisible by 3.
If $n = 3k+1$ then $n+2 = 3k+3$ is divisible by 3.
If $n = 3k+2$ then $n+4 = 3k+6$ is divisible by 3.

Solution 4.3

Each of these numbers has three or more ways of being written as a sum of two odd primes. We give just one way:

$40 = 3 + 37$
$42 = 5 + 37$
$44 = 3 + 41$
$46 = 23 + 23$
$48 = 5 + 43$
$50 = 19 + 31$
$52 = 5 + 47$
$54 = 23 + 31$
$56 = 19 + 37$
$58 = 17 + 41$
$60 = 7 + 53$

Solution 5.1

The multiples of 3 are F_4, F_8, F_{12}, F_{16} and F_{20}. It appears that every fourth term is a multiple of 3. Similarly, every third term — and these alone — appear to be multiples of 2, and every fifth term is a multiple of 5.

Solution 5.2

Let $a = q_1n + r$ and $b = q_2n + s$. Now let t be the remainder when $r + s$ is divided by n; that is,

$$r + s = q_3n + t; \quad 0 \leq t < n$$

for some integer q_3. Adding the first two equations gives

$$\begin{aligned} a + b &= q_1n + q_2n + r + s \\ &= q_1n + q_2n + q_3n + t \\ &= (q_1 + q_2 + q_3)n + t. \end{aligned}$$

Hence, by the uniqueness of remainder, t is also the remainder on dividing $a + b$ by n.

Solution 5.3

(a) The remainder sequence on dividing by 6 begins:

$$1, 1, 2, 3, 5, 2, 1, 3, 4, 1, 5, 0, 5, 5, 4, 3, 1, 4, 5, 3, 2, 5, 1, 0, 1, 1, \ldots.$$

The sequence repeats after 24 terms and the zeros occur at terms 12 and 24. Hence every twelfth term of the Fibonacci sequence is divisible by 6.

(b) The remainder sequence on dividing by 7 begins:

$$1, 1, 2, 3, 5, 1, 6, 0, 6, 6, 5, 4, 2, 6, 1, 0, 1, 1, \ldots,$$

repeating after 16 terms, so zeros occur every eighth term and these correspond to the Fibonacci numbers which are divisible by 7.

Solution 5.4

Suppose that F_n is the first multiple of a in the Fibonacci sequence and that F_m is any other multiple of a. Let $m = nq + r$, where $0 \leq r < n$. Then, if $r \neq 0$ we can apply the 'useful relationship' and write

$$F_m = F_{nq+r} = F_{nq-1}F_r + F_{nq}F_{r+1}.$$

Now a divides both F_m and F_{nq}, (the latter by Theorem 5.2) and so a divides $F_{nq-1}F_r$.

But from $\gcd(F_{nq-1}, F_{nq}) = 1$, and the fact that a divides F_{nq}, it follows that $\gcd(a, F_{nq-1}) = 1$. Since a divides $F_{nq-1}F_r$, Euclid's Lemma now gives that a divides F_r.

Finally, as $0 < r < n$ and F_n is the first multiple of a, we have a contradiction. So $r = 0$. Hence $m = nq$ and m is a multiple of n.

Solution 5.5

$F_8 = 21$ is divisible by 7
$F_{10} = 55$ is divisible by 11
$F_{14} = 377$ is divisible by 13
$F_{18} = 2584$ is divisible by both 17 and 19.

Solution 5.6

$F_{n+1}F_n - F_nF_{n-1} = F_n(F_{n+1} - F_{n-1}) = F_n^2$, for $n \geq 2$.

Therefore

$$\begin{aligned} &F_1^2 + F_2^2 + F_3^2 + F_4^2 + \cdots + F_n^2 \\ &= F_1^2 + (F_3F_2 - F_2F_1) + (F_4F_3 - F_3F_2) \\ &\quad + (F_5F_4 - F_4F_3) + \cdots + (F_{n+1}F_n - F_nF_{n-1}) \\ &= F_1^2 - F_2F_1 + F_{n+1}F_n, \quad \text{all other terms cancelling,} \\ &= F_{n+1}F_n, \quad \text{since } F_1 = F_2 = 1. \end{aligned}$$

This result lends itself to a simple induction proof, but here we were asked to deduce it from the earlier property.

SOLUTIONS TO ADDITIONAL EXERCISES

Section 1

1 As

$$20! = 1 \times 2 \times 3 \times 4 \times \cdots \times 19 \times 20$$

it is divisible by each of the primes from 2 to 19 inclusive, and by no others.

Looking at the terms on the right-hand side, the primes from 11 to 19 occur just once. The prime 7 occurs twice, in the terms 7 and 14. The prime 5 occurs in terms 5, 10, 15 and 20. The prime 3 occurs once in each term 3, 6, 12, and 15 but twice in terms 9 and 18, making eight occurrences in all. Finally, the prime 2 occurs once in terms 2, 6, 10, 14 and 18, twice in terms 4, 12 and 20, three times in term 8 and four times in term 16, making a total of eighteen occurrences. Hence

$$20! = 2^{18} \times 3^8 \times 5^4 \times 7^2 \times 11 \times 13 \times 17 \times 19.$$

2 Since pq divides a^n, we know that p divides a^n and Euclid's Lemma gives p divides a. Similarly, q divides a^n and so q divides a. Now as p and q are distinct primes, $\gcd(p, q) = 1$ and so pq divides a; say $(pq)r = a$. But then, raising to the nth power, $(pq)^n r^n = a^n$ which confirms that $(pq)^n$ divides a^n.

3 Suppose that $3p + 1$ is a square, say $3p + 1 = n^2$. Then

$$3p = n^2 - 1 = (n-1)(n+1).$$

Now $n > 2$, since $p \geq 2$, and so the right-hand side of this equation is a product of two divisors each exceeding 1. The left-hand side is the product of two primes. By uniqueness of prime decomposition we must have either $3 = n - 1$ and $p = n + 1$, or alternatively $3 = n + 1$ and $p = n - 1$. The former case leads to $n = 4$ and $p = 5$ which is one solution. The latter case leads to $n = 2$ and $p = 1$, which is invalid.

4 Thinking in terms of remainders on division by 3, there are three possibilities for the prime p. It is 3, of form $3k+1$, or of form $3k+2$.

If $p=3$ then $8p+1=25$ is composite.
If $p=3k+1$ then $8p+1=24k+9=3(8k+3)$ is composite.
If $p=3k+2$ then $8p-1=24k+15=3(8k+5)$ is composite.

5 The prime p must take one of the twelve forms $12k+r$, where $0 \leq r \leq 11$. However, when r is even $12k+r$ is divisible by 2, and similarly $12k+r$ is divisible by 3 when $r=3$ or 9. The only remaining possibilities are $12k+1$, $12k+5$, $12k+7$ and $12k+11$, and any prime $p \geq 5$ must take one of these forms.

We are told that $p \geq 5$ so $p=2$ and $p=3$ are not possibilities.

Now

$$\begin{aligned} (12k+1)^2 &= 24\left(6k^2+k\right)+1, \\ (12k+5)^2 &= 24\left(6k^2+5k+1\right)+1, \\ (12k+7)^2 &= 24\left(6k^2+7k+2\right)+1, \\ \text{and} \qquad (12k+11)^2 &= 24\left(6k^2+11k+5\right)+1. \end{aligned}$$

So whichever of the four forms p takes, p^2 is of the form $24m+1$.

If q is another such prime, say $q^2=24n+1$, then

$$p^2-q^2=(24m+1)-(24n+1)=24(m-n)$$

is divisible by 24.

6 Consider the given factorization

$$a^n-1=(a-1)(a^{n-1}+a^{n-2}+a^{n-3}+\cdots+a+1).$$

For a^n-1 to be prime one of the two divisors on the right-hand side of this equation will have to be equal to 1. The only way this can happen is when $a-1=1$, so that $a=2$.

Next, suppose that n is composite, say $n=rs$, where $r>1$ and $s>1$. Then $2^n-1=(2^r)^s-1$, and so replacing a by 2^r and replacing n by s in the above factorization:

$$(2^r)^s-1=(2^r-1)(2^{r(s-1)}+2^{r(s-2)}+2^{r(s-3)}+\cdots+2^r+1).$$

Once again this expresses 2^n-1 as a product of two divisors and, this time, since $2^r>2$ neither divisor is equal to 1. This contradicts the primality of 2^n-1. The only assumption we have made is that $n=rs$ is composite. Hence we conclude that n must be prime.

Section 2

1 First we have the factorization

$$n=3344=2^4\times 11\times 19.$$

For each prime which divides either m or n, we take the lesser exponent to get $\gcd(m,n)$ and the greater exponent to get $\operatorname{lcm}(m,n)$. Therefore

$$\gcd\left(2^3\times 3^2\times 7\times 11,\ 2^4\times 11\times 19\right)=2^3\times 11$$

and

$$\operatorname{lcm}\left(2^3\times 3^2\times 7\times 11,\ 2^4\times 11\times 19\right)=2^4\times 3^2\times 7\times 11\times 19.$$

2 The integer 8 can be written as a product of non-trivial divisors in three ways, namely $2 \times 2 \times 2$, 2×4 and 8. Accordingly, numbers with each of the following prime decompositions will have exactly eight divisors:

$$p \times q \times r,\ p \times q^3,\ p^7, \quad \text{where } p,\ q \text{ and } r \text{ are any distinct primes.}$$

As $2^7 = 128$ all numbers of form p^7 exceed 100. Those of the other forms which do not exceed 100 are

$$2 \times 3 \times 5 = 30,\ 2 \times 3 \times 7 = 42,\ 2 \times 3 \times 11 = 66,\ 2 \times 3 \times 13 = 78,\ 2 \times 5 \times 7 = 70,$$
$$2^3 \times 3 = 24,\ 2^3 \times 5 = 40,\ 2^3 \times 7 = 56,\ 2^3 \times 11 = 88,\ 3^3 \times 2 = 54.$$

3 (a) The integer 6 is practical. The numbers 1 to 6 respectively are expressed as sums of distinct divisors as

$$1,\ 2,\ 3,\ 1+3,\ 2+3,\ 6.$$

10 is not practical. Its divisors are 1, 2, 5 and 10, but 4 cannot be expressed as a sum of these without repeats.

12 is practical. The numbers 1 to 12 are sums of divisors as follows:

$$1,\ 2,\ 3,\ 1+3,\ 2+3,\ 6,\ 1+6,\ 2+6,\ 3+6,\ 1+3+6,\ 2+3+6,\ 12.$$

14 is not practical. 4 cannot be expressed as a sum of numbers from $\{1, 2, 7, 14\}$ with no repeats.

16 is practical. The numbers 1 to 8 are given, respectively, by

$$1,\ 2,\ 1+2,\ 4,\ 1+4,\ 2+4,\ 1+2+4,\ 8.$$

The numbers from 9 to 15 are obtained by adding the divisor 8 to the first seven of the above expressions. 16 is just itself.

(b) The demonstration that 16 is a practical number reveals a pattern which will persist for any power of 2. But to make it 'watertight' we shall appeal to induction.

Let $P(n)$ be the statement that every integer in the range 1 to $2^n - 1$ can be written as a sum of distinct members of the set $\{1, 2, 2^2, 2^3, \ldots, 2^{n-1}\}$. (This is equivalent to what is required; we have just excluded the obvious case of 2^n itself being written as the divisor 2^n.)

The basis for induction is immediate as $P(1)$ claims no more than that 1 can be written as a sum of members of $\{1\}$.

For the induction step, suppose that $P(k)$ is true and let m be any integer in the range 1 to $2^{k+1} - 1$. If $m < 2^k$ then the induction hypothesis tells us that it is a sum of distinct members of

$$\{1,\ 2,\ 2^2,\ 2^3, \ldots, 2^{k-1}\}$$

and there is nothing to prove. On the other hand, if $m \geq 2^k$ then $m - 2^k < 2^k$ and the induction hypothesis tells us that $m - 2^k$ can be written as a sum of distinct members of the set

$$\{1,\ 2,\ 2^2,\ 2^3, \ldots, 2^{k-1}\}.$$

Addition of 2^k then gives m written as a sum of distinct members of the set

$$\{1,\ 2,\ 2^2,\ 2^3, \ldots, 2^{k-1},\ 2^k\},$$

showing the truth of $P(k+1)$.

Hence, by Mathematical Induction, $P(n)$ is true for all integers $n \geq 1$.

Section 3

1 Suppose that $p_1, p_2, p_3, \ldots, p_n$ are the only primes. Consider $N = p_1 + p_2p_3 \ldots p_n$. If p_1 divides N, then p_1 divides $N - p_1$. That is p_1 divides $p_2p_3 \ldots p_n$. The Corollary to Euclid's Lemma now gives $p_1 = p_i$ for some $2 \leq i \leq n$, which is a contradiction.

Similarly, if p_i divides N for some $2 \leq i \leq n$, then p_i divides $(N - p_2p_3 \ldots p_n)$; that is p_i divides p_1, which is impossible.

Hence N is not divisible by any of the primes $p_1, p_2, p_3, \ldots, p_n$.

This amounts to an alternative proof of the infinitude of the primes. It shows that there cannot be just n primes because, from such a list of n primes, we can always construct another prime; the number N has to be divisible by some prime but not one of the primes in the 'list'.

2 Suppose that p, $p + d$ and $p + 2d$ are three primes, where $p > 3$.

We first note that d must be even because otherwise one of p or $p + d$ would be even, contrary to the fact that they are odd primes.

In a similar way d must be divisible by 3 because otherwise one of $p + d$ or $p + 2d$ is divisible by 3, contrary to the fact that they are primes. The following table illustrates why this is so. The prime $p > 3$ must be one of the forms $3k + 1$ or $3k + 2$ and each possibility $d = 3r + 1$ or $3r + 2$ leads to either $p + d$ or $p + 2d$ being divisible by 3.

	$d = 3r + 1$	$d = 3r + 2$
$p = 3k + 1$	$p + 2d = 3(k + 2r + 1)$	$p + d = 3(k + r + 1)$
$p = 3k + 2$	$p + d = 3(k + r + 1)$	$p + 2d = 3(k + 2r + 2)$

We conclude that d is divisible by both 2 and 3 and hence by 6.

For five primes in arithmetic progression, p, $p + d$, $p + 2d$, $p + 3d$ and $p + 4d$, we have already shown that d is divisible by 6. A repeat of the above argument shows that if d is not a multiple of 5, then one of the five numbers must be divisible by 5. Of course $p = 5$ is now possible, and indeed $p = 5$, $d = 6$ gives the arithmetic progression 5, 11, 17, 23, 29 of five primes. When $p > 5$ we must have that d is divisible by both 6 and 5 and, as $\gcd(5, 6) = 1$, d is a multiple of 30.

3 Successive terms of the given sequence are $n^2 + 3$ and $(n + 1)^2 + 3$. Let d be the greatest common divisor of these two numbers. Then

$$d \mid \left((n+1)^2 + 3 - \left(n^2 + 3\right)\right); \text{ that is } d \mid 2n + 1.$$

We repeatedly use that fact that, if d divides two numbers, then it divides any integer combination of them.

Therefore

$$d \mid \left(n(2n+1) - 2\left(n^2 + 3\right)\right); \text{ that is } d \mid n - 6.$$

Therefore

$$d \mid (2n + 1 - 2(n - 6)); \text{ that is } d \mid 13.$$

Hence $\gcd\left(n^2 + 3, (n+1)^2 + 3\right) = 1$ or 13.

Section 4

1 Any number is of one of the forms $12k+r$, $0 \leq r \leq 11$. To be a prime (excluding the primes 2 and 3), r must take one of the values 1, 5, 7 or 11. But $p+2$ is also prime. This eliminates the possibility $r=1$ for which $p+2=12k+3$ which is divisible by 3. It also eliminates $r=7$ which gives $p+2=12k+9$, again divisible by 3. The remaining possibilities are:

See Additional Exercise 5 of Section 1.

$$p = 12k+5, \quad p+2 = 12k+7;$$

giving

$$p+(p+2) = 24k+12,$$

and

$$p = 12k+11, \quad p+2 = 12k+13;$$

giving

$$p+(p+2) = 24k+24.$$

In both cases the sum of the twin primes is divisible by 12.

2 Consider the five consecutive odd integers n, $n+2$, $n+4$, $n+6$ and $n+8$. One of these numbers is divisible by 5 (see Additional Exercise 2 of Section 3) and, of any three in succession, one is divisible by 3. So, for $n > 5$, n, $n+2$, $n+6$ and $n+8$ can all be prime only when $n+4$ is divisible by both 3 and 5 (and therefore by 15). So $n+4 = 15k$, giving $n = 15k-4 = 15(k-1)+11$, and the required remainder is 11.

3 Suppose that Goldbach's Conjecture holds. Then, for any $n \geq 4$, $2n-2 \geq 6$ and so can be written as a sum of two odd primes, say $2n-2 = p_1 + p_2$. Hence

$$2n = p_1 + p_2 + 2 \quad \text{and} \quad 2n+1 = p_1 + p_2 + 3,$$

showing that $2n$ and $2n+1$ can be written as the sum of three primes. Therefore all integers from 8 onwards can be written in this form. The two remaining integers 6 and 7 can also be expressed as a sum of three primes since

$$6 = 2+2+2 \quad \text{and} \quad 7 = 2+2+3.$$

Conversely, suppose that every integer greater than or equal to 6 can be written as the sum of three primes and consider the even integer $2n$, for $n \geq 3$.

We know that

$$2n+2 = p_1 + p_2 + p_3,$$

where p_1, p_2 and p_3 are prime.

But p_1, p_2 and p_3 cannot all be odd for, if so, the sum on the right-hand side is odd. So one of the p_i is 2; say $p_3 = 2$. In this case

$$2n = p_1 + p_2.$$

Finally if either of p_1 or p_2 is 2, then, as $p_1 + p_2$ is even, so too is the other contradicting the fact that $n \geq 3$.

Hence $2n$ is expressed as the sum of two odd primes, which is Goldbach's conjecture.

4 The even integers take one of the five forms $10k$, $10k+2$, $10k+4$, $10k+6$ or $10k+8$. We can write each of these as the sum of two composite numbers as follows:

$$\begin{aligned} 10k &= 15 + (10k - 15), \quad && k \geq 3; \\ 10k+2 &= 27 + (10k - 25), && k \geq 4; \\ 10k+4 &= 9 + (10k - 5), && k \geq 2; \\ 10k+6 &= 21 + (10k - 15), && k \geq 3; \\ 10k+8 &= 33 + (10k - 25), && k \geq 4. \end{aligned}$$

The second term in each sum is divisible by 5 and hence is composite provided it exceeds 5, however the given condition on k ensures this. Note that 38 is the largest even number which cannot be expressed in this way.

Section 5

1

$$\begin{aligned} F_{22} &= F_{11+11} = F_{10}F_{11} + F_{11}F_{12} = F_{11}(F_{10} + F_{12}) \\ &= 89(55 + 144) = 17\,711. \\ F_{23} &= F_{12+11} = F_{11}F_{11} + F_{12}F_{12} \\ &= 89^2 + 144^2 = 28\,657. \\ F_{24} &= F_{22} + F_{23} = 17\,711 + 28\,657 = 46\,368. \\ F_{22} &= 89 \times 199 = F_{11} \times 199. \\ F_{24} &= 46\,368 = F_4 \times 15\,456 = F_6 \times 5796 = F_8 \times 2208 = F_{12} \times 322. \end{aligned}$$

2 (a) $F_7 = 13$ and hence, by Theorem 5.2 and Problem 5.4, F_n is a multiple of 13 if, and only if, n is a multiple of 7. Therefore, the multiples of 13 occur every seventh term.

(b) As $F_6 = 8$ the multiples of 8 occur every sixth term. The first multiple of 4 which is a Fibonacci number is also $F_6 = 8$. So the multiples of 4 also occur every sixth term.

3 (a) The identity

$$F_1 + F_2 + F_3 + \cdots + F_n = F_{n+2} - 1$$

is readily seen by adding the equations in the system

$$\begin{aligned} F_1 &= F_3 - F_2 \\ F_2 &= F_4 - F_3 \\ F_3 &= F_5 - F_4 \\ &\vdots \\ F_n &= F_{n+2} - F_{n+1} \end{aligned}$$

and noting that all the terms on the right cancel except $F_{n+2} - F_2$. The fact that $F_2 = 1$ completes the argument.

A rather more formal proof is given by Mathematical Induction.

Let $P(n)$ be the claim of the identity.

Putting in values for $n = 1$ we get

$$1 = 2 - 1,$$

which is true, providing the basis for induction.

So suppose $P(k)$ is true, for some $k \geq 1$; that is,

$$F_1 + F_2 + F_3 + \cdots + F_k = F_{k+2} - 1.$$

Adding F_{k+1} to both sides gives

$$\begin{aligned} F_1 + F_2 + F_3 + \cdots + F_k + F_{k+1} &= F_{k+1} + F_{k+2} - 1 \\ &= F_{k+3} - 1, \end{aligned}$$

completing the induction step.

(b) Again, proof by Mathematical Induction is straightforward. The result is true for $n = 1$ since it asserts that $F_1 = F_2$. The assumption of its truth for $n = k$, namely,

$$F_1 + F_3 + F_5 + \cdots + F_{2k-1} = F_{2k}$$

leads immediately to

$$F_1 + F_3 + F_5 + \cdots + F_{2k-1} + F_{2k+1} = F_{2k} + F_{2k+1} = F_{2k+2},$$

this being the claim for $n = k + 1$.

(c) Take the two equations

$$\begin{aligned} F_1 + F_2 + F_3 + \cdots + F_{2n} &= F_{2n+2} - 1, \\ F_1 + F_3 + F_5 + \cdots + F_{2n-1} &= F_{2n} \end{aligned}$$

established in parts (a) and (b). Subtraction gives

$$\begin{aligned} F_2 + F_4 + F_6 + \cdots + F_{2n} &= F_{2n+2} - F_{2n} - 1 \\ &= F_{2n+1} + F_{2n} - F_{2n} - 1 \\ &= F_{2n+1} - 1. \end{aligned}$$

4 (a) $$\begin{aligned} F_{n+1}^2 - F_{n-1}^2 &= (F_{n+1} - F_{n-1})(F_{n+1} + F_{n-1}) \\ &= F_n(F_n + 2F_{n-1}), \quad \text{using } F_{n+1} = F_n + F_{n-1}. \end{aligned}$$

Now if 2 divides F_n, then 2 divides $F_n + 2F_{n-1}$, and so 4 divides $F_{n+1}^2 - F_{n-1}^2$.

(b) $$\begin{aligned} F_{n+1}^3 - F_{n-1}^3 &= (F_{n+1} - F_{n-1})\left(F_{n+1}^2 + F_{n+1}F_{n-1} + F_{n-1}^2\right) \\ &= F_n\left((F_n + F_{n-1})^2 + (F_n + F_{n-1})F_{n-1} + F_{n-1}^2\right), \\ &\qquad \text{using } F_{n+1} = F_n + F_{n-1}, \\ &= F_n\left(F_n^2 + 3F_nF_{n-1} + 3F_{n-1}^2\right). \end{aligned}$$

Now if 3 divides F_n, then 3 divides $F_n^2 + 3F_nF_{n-1} + 3F_{n-1}^2$, and so 9 divides $F_{n+1}^3 - F_{n-1}^3$.

5 Let $P(n)$ be the claim that, for $n \geq 3$, each integer from 1 up to $F_n - 1$ can be written as a sum of one or more distinct Fibonacci numbers from the set $\{F_1, F_2, \ldots, F_{n-1}\}$.

For the case $n = 3$, $F_3 - 1 = 1$ and the only number in the range 1 to $F_3 - 1$ is 1 itself. But $1 = F_1$, providing the basis for induction.

With the Second Principle of Mathematical Induction in mind, suppose that each of $P(3)$, $P(4)$, …, $P(k)$ is true and consider $P(k + 1)$. Let m be any integer in the range $1 \leq m < F_{k+1}$. If $m < F_k$ then, by $P(k)$, m can be written as a sum of distinct Fibonacci numbers from the set $\{F_1, F_2, \ldots, F_{k-1}\}$.

On the other hand, if $m \geq F_k$ then either $m = F_k$, in which case it is a sum of one Fibonacci number, or $m > F_k$. In this latter case

$$m - F_k < F_{k+1} - F_k = F_{k-1}$$

and so, by $P(k - 1)$, $m - F_k$ can be written as a sum of distinct Fibonacci numbers from the set $\{F_1, F_2, \ldots, F_{k-2}\}$. By adding F_k to both sides, m is then written as a sum of distinct Fibonacci numbers from the set $\{F_1, F_2, \ldots, F_{k-2}, F_k\}$.

In all cases m is a sum of distinct members from the set $\{F_1, F_2, F_3, \ldots, F_k\}$, which is $P(k + 1)$.

This completes the induction proof.

APPENDIX: TABLE OF PRIMES

The following table lists all the odd integers up to 3999, excluding the multiples of 5. The entry ‘P’ in the table indicates that the number is prime. Otherwise the smallest prime divisor of the number is given. The numbers are arranged in blocks of 100, with the units digit at the head of the column and the numbers of 10’s in the left-hand column.

	1	3	7	9		1	3	7	9		1	3	7	9		1	3	7	9
0		P	P	3	50	3	P	3	P	100	7	17	19	P	150	19	3	11	3
1	P	P	P	P	51	7	3	11	3	101	3	P	3	P	151	P	17	37	7
2	3	P	3	P	52	P	P	17	23	102	P	3	13	3	152	3	P	3	11
3	P	3	P	3	53	3	13	3	7	103	P	P	17	P	153	P	3	29	3
4	P	P	P	7	54	P	3	P	3	104	3	7	3	P	154	23	P	7	P
5	3	P	3	P	55	19	7	P	13	105	P	3	7	3	155	3	P	3	P
6	P	3	P	3	56	3	P	3	P	106	P	P	11	P	156	7	3	P	3
7	P	P	7	P	57	P	3	P	3	107	3	29	3	13	157	P	11	19	P
8	3	P	3	P	58	7	11	P	19	108	23	3	P	3	158	3	P	3	7
9	7	3	P	3	59	3	P	3	P	109	P	P	P	7	159	37	3	P	3
10	P	P	P	P	60	P	3	P	3	110	3	P	3	P	160	P	7	P	P
11	3	P	3	7	61	13	P	P	P	111	11	3	P	3	161	3	P	3	P
12	11	3	P	3	62	3	7	3	17	112	19	P	7	P	162	P	3	P	3
13	P	7	P	P	63	P	3	7	3	113	3	11	3	17	163	7	23	P	11
14	3	11	3	P	64	P	P	P	11	114	7	3	31	3	164	3	31	3	17
15	P	3	P	3	65	3	P	3	P	115	P	P	13	19	165	13	3	P	3
16	7	P	P	13	66	P	3	23	3	116	3	P	3	7	166	11	P	P	P
17	3	P	3	P	67	11	P	P	7	117	P	3	11	3	167	3	7	3	23
18	P	3	11	3	68	3	P	3	13	118	P	7	P	29	168	41	3	7	3
19	P	P	P	P	69	P	3	17	3	119	3	P	3	11	169	19	P	P	P
20	3	7	3	11	70	P	19	7	P	120	P	3	17	3	170	3	13	3	P
21	P	3	7	3	71	3	23	3	P	121	7	P	P	23	171	29	3	17	3
22	13	P	P	P	72	7	3	P	3	122	3	P	3	P	172	P	P	11	7
23	3	P	3	P	73	17	P	11	P	123	P	3	P	3	173	3	P	3	37
24	P	3	13	3	74	3	P	3	7	124	17	11	29	P	174	P	3	P	3
25	P	11	P	7	75	P	3	P	3	125	3	7	3	P	175	17	P	7	P
26	3	P	3	P	76	P	7	13	P	126	13	3	7	3	176	3	41	3	29
27	P	3	P	3	77	3	P	3	19	127	31	19	P	P	177	7	3	P	3
28	P	P	7	17	78	11	3	P	3	128	3	P	3	P	178	13	P	P	P
29	3	P	3	13	79	7	13	P	17	129	P	3	P	3	179	3	11	3	7
30	7	3	P	3	80	3	11	3	P	130	P	P	P	7	180	P	3	13	3
31	P	P	P	11	81	P	3	19	3	131	3	13	3	P	181	P	7	23	17
32	3	17	3	7	82	P	P	P	P	132	P	3	P	3	182	3	P	3	31
33	P	3	P	3	83	3	7	3	P	133	11	31	7	13	183	P	3	11	3
34	11	7	P	P	84	29	3	7	3	134	3	17	3	19	184	7	19	P	43
35	3	P	3	P	85	23	P	P	P	135	7	3	23	3	185	3	17	3	11
36	19	3	P	3	86	3	P	3	11	136	P	29	P	37	186	P	3	P	3
37	7	P	13	P	87	13	3	P	3	137	3	P	3	7	187	P	P	P	P
38	3	P	3	P	88	P	P	P	7	138	P	3	19	3	188	3	7	3	P
39	17	3	P	3	89	3	19	3	29	139	13	7	11	P	189	31	3	7	3
40	P	13	11	P	90	17	3	P	3	140	3	23	3	P	190	P	11	P	23
41	3	7	3	P	91	P	11	7	P	141	17	3	13	3	191	3	P	3	19
42	P	3	7	3	92	3	13	3	P	142	7	P	P	P	192	17	3	41	3
43	P	P	19	P	93	7	3	P	3	143	3	P	3	P	193	P	P	13	7
44	3	P	3	P	94	P	23	P	13	144	11	3	P	3	194	3	29	3	P
45	11	3	P	3	95	3	P	3	7	145	P	P	31	P	195	P	3	19	3
46	P	P	P	7	96	31	3	P	3	146	3	7	3	13	196	37	13	7	11
47	3	11	3	P	97	P	7	P	11	147	P	3	7	3	197	3	P	3	P
48	13	3	P	3	98	3	P	3	23	148	P	P	P	P	198	7	3	P	3
49	P	17	7	P	99	P	3	P	3	149	3	P	3	P	199	11	P	P	P

	1	3	7	9		1	3	7	9		1	3	7	9		1	3	7	9
200	3	P	3	7	250	41	P	23	13	300	P	3	31	3	350	3	31	3	11
201	P	3	P	3	251	3	7	3	11	301	P	23	7	P	351	P	3	P	3
202	43	7	P	P	252	P	3	7	3	302	3	P	3	13	352	7	13	P	P
203	3	19	3	P	253	P	17	43	P	303	7	3	P	3	353	3	P	3	P
204	13	3	23	3	254	3	P	3	P	304	P	17	11	P	354	P	3	P	3
205	7	P	11	29	255	P	3	P	3	305	3	43	3	7	355	53	11	P	P
206	3	P	3	P	256	13	11	17	7	306	P	3	P	3	356	3	7	3	43
207	19	3	31	3	257	3	31	3	P	307	37	7	17	P	357	P	3	7	3
208	P	P	P	P	258	29	3	13	3	308	3	P	3	P	358	P	P	17	37
209	3	7	3	P	259	P	P	7	23	309	11	3	19	3	359	3	P	3	59
210	11	3	7	3	260	3	19	3	P	310	7	29	13	P	360	13	3	P	3
211	P	P	29	13	261	7	3	P	3	311	3	11	3	P	361	23	P	P	7
212	3	11	3	P	262	P	43	37	11	312	P	3	53	3	362	3	P	3	19
213	P	3	P	3	263	3	P	3	7	313	31	13	P	43	363	P	3	P	3
214	P	P	19	7	264	19	3	P	3	314	3	7	3	47	364	11	P	7	41
215	3	P	3	17	265	11	7	P	P	315	23	3	7	3	365	3	13	3	P
216	P	3	11	3	266	3	P	3	17	316	29	P	P	P	366	7	3	19	3
217	13	41	7	P	267	P	3	P	3	317	3	19	3	11	367	P	P	P	13
218	3	37	3	11	268	7	P	P	P	318	P	3	P	3	368	3	29	3	7
219	7	3	13	3	269	3	P	3	P	319	P	31	23	7	369	P	3	P	3
220	31	P	P	47	270	37	3	P	3	320	3	P	3	P	370	P	7	11	P
221	3	P	3	7	271	P	P	11	P	321	13	3	P	3	371	3	47	3	P
222	P	3	17	3	272	3	7	3	P	322	P	11	7	P	372	61	3	P	3
223	23	7	P	P	273	P	3	7	3	323	3	53	3	41	373	7	P	37	P
224	3	P	3	13	274	P	13	41	P	324	7	3	17	3	374	3	19	3	23
225	P	3	37	3	275	3	P	3	31	325	P	P	P	P	375	11	3	13	3
226	7	31	P	P	276	11	3	P	3	326	3	13	3	7	376	P	53	P	P
227	3	P	3	43	277	17	47	P	7	327	P	3	29	3	377	3	7	3	P
228	P	3	P	3	278	3	11	3	P	328	17	7	19	11	378	19	3	7	3
229	29	P	P	11	279	P	3	P	3	329	3	37	3	P	379	17	P	P	29
230	3	7	3	P	280	P	P	7	53	330	P	3	P	3	380	3	P	3	13
231	P	3	7	3	281	3	29	3	P	331	7	P	31	P	381	37	3	11	3
232	11	23	13	17	282	7	3	11	3	332	3	P	3	P	382	P	P	43	7
233	3	P	3	P	283	19	P	P	17	333	P	3	47	3	383	3	P	3	11
234	P	3	P	3	284	3	P	3	7	334	13	P	P	17	384	23	3	P	3
235	P	13	P	7	285	P	3	P	3	335	3	7	3	P	385	P	P	7	17
236	3	17	3	23	286	P	7	47	19	336	P	3	7	3	386	3	P	3	53
237	P	3	P	3	287	3	13	3	P	337	P	P	11	31	387	7	3	P	3
238	P	P	7	P	288	43	3	P	3	338	3	17	3	P	388	P	11	13	P
239	3	P	3	P	289	7	11	P	13	339	P	3	43	3	389	3	17	3	7
240	7	3	29	3	290	3	P	3	P	340	19	41	P	7	390	47	3	P	3
241	P	19	P	41	291	41	3	P	3	341	3	P	3	13	391	P	7	P	P
242	3	P	3	7	292	23	37	P	29	342	11	3	23	3	392	3	P	3	P
243	11	3	P	3	293	3	7	3	P	343	47	P	7	19	393	P	3	31	3
244	P	7	P	31	294	17	3	7	3	344	3	11	3	P	394	7	P	P	11
245	3	11	3	P	295	13	P	P	11	345	7	3	P	3	395	3	59	3	37
246	23	3	P	3	296	3	P	3	P	346	P	P	P	P	396	17	3	P	3
247	7	P	P	37	297	P	3	13	3	347	3	23	3	7	397	11	29	41	23
248	3	13	3	19	298	11	19	29	7	348	59	3	11	3	398	3	7	3	P
249	47	3	11	3	299	3	41	3	P	349	P	7	13	P	399	13	3	7	3

INDEX

Li(x) 25
max$\{a, b\}$ 13
min$\{a, b\}$ 12
$\pi(x)$ 25
$\tau(n)$ 13

Bertrand's conjecture 16

composite 5
consecutive composite integers 23
Corollary to Euclid's Lemma 9

density of primes 25
Dirichlet's theorem 19
divisors of an integer 11

Euclid's Lemma for prime divisors 8
Euclid's theorem 15

Fibonacci numbers 27
Fibonacci numbers, divisibility property 31
Fibonacci numbers, relative primeness of consecutive numbers 29
Fibonacci primes 28
Fibonacci sequence 27
formula for $\tau(n)$ 13
function τ 13
fundamental theorem of arithmetic 10

Goldbach's conjecture 24

prime 5
prime decomposition 10
prime decomposition of gcd(m, n) 12
prime decomposition of lcm(m, n) 13
prime number theorem 26
prime quartets 24
prime triplets 24
primes generated by polynomials 20
primes in arithmetic progression 16
primes of the form $4k + 3$ 18

sieve of Eratosthenes 7
size of the nth prime 15

twin primes 22

value of gcd(n, p) 8